ALLPLEX Access Easy Master Controller

Software Manual

BOSCH

en Software Manual

All rights reserved. No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of BOSCH SECURITY SYSTEMS.

This manual is provided pursuant to a license agreement containing restrictions on their use. The manual contains valuable trade secrets and proprietary information of BOSCH SECURITY SYSTEMS and is protected by international copyright law. It may not be copied or distributed to third parties, or used in any manner not provided for in the said license agreement.

All software is provided "AS IS." The sole obligation of BOSCH SECURITY SYSTEMS shall be to make available all published modifications that correct program problems are published within one (1) year from the date of shipment.

The software is intended for use only with the hardware specified in this manual and in the absence of other software. Concurrent use with other software or with hardware not specified may cause the program to function improperly or not at all. BOSCH SECURITY SYSTEMS may not provide support for systems operating under such conditions.

All efforts have been made to ensure the accuracy of the contents of this manual.
The above notwithstanding, BOSCH SECURITY SYSTEMS assume no responsibility for any errors in this manual or their consequences.

The information on this document is subject to change without notice.

Access Easy Master Controller™ is a trademark of Bosch Security Systems
Other product and company names mentioned herein may be the trademarks of their respective owner.

End-User License Agreement for Access Easy Master Controller™ software

---

BOSCH SECURITY SYSTEMS SOFTWARE PRODUCTS: -

Server Software: Access Easy Master Controller™ Software

BOSCH SECURITY SYSTEMS HARDWARE PRODUCTS: Access Easy Master Controller™ and all input/output modules.

IMPORTANT - READ CAREFULLY: This End User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and BOSCH SECURITY SYSTEMS for the BOSCH SECURITY SYSTEMS SOFTWARE PRODUCT, which you acquired, and any of the HARDWARE PRODUCT(s) identified above.

The SOFTWARE PRODUCT includes computer software, the associate media, any printed materials, and any "online" or electronic documentation. By installing, copying or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, BOSCH SECURITY SYSTEMS or its resellers are unwilling to license the SOFTWARE PRODUCT to you. In such event, you may not use or copy the SOFTWARE PRODUCT, and you should promptly contact BOSCH SECURITY SYSTEMS or its distributors for instructions on return of the unused product for a refund.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as intellectual property laws and treaties.

The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. The SOFTWARE PRODUCT refers to the Access Easy Master Controller™ Software that runs on the "Access Easy Master Controller™ that enables a computer or workstation running a Web Browser Software ("Third Party Software") to access or utilise the services provided by the Access Easy Master Controller™ Access control. This EULA grants to you the following rights to the SOFTWARE PRODUCT:

- Use of the Server Software. You may use one copy of the Server Software running on one Server, which may be connected at any point in time an unlimited number of workstations or computers operating on one or more networks. You must acquire a separate Client Application Software License to access or otherwise utilise the services of the Server by using the Third Party Software.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATION

- Client Access Licenses. This EULA grants you the number of Client Access Licenses for the SOFTWARE PRODUCT indicated at the top of this EULA. Each licenses permits one additional computer or workstation the right to access or utilise the services of the Server. The services of the Server are considered to have accessed or utilised when there is a direct or indirect connection between a computer or workstation and a Server.

- Restriction against copying or modifying the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is copyrighted by BOSCH SECURITY SYSTEMS or third parties. Except as expressly permitted in this agreement, you may not copy or otherwise reproduce the SOFTWARE PRODUCT. In no event does the limited copying or reproduction permitted under this agreement include the right to de-compile, reverse engineering, disassemble, modify or electronically transfer the SOFTWARE PRODUCT, or to translate the SOFTWARE PRODUCT into another computer language.

- Separation of Components. The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one Server.

- Rental. You may not rent or lease the SOFTWARE PRODUCT.

- Termination. Without prejudice to any other rights, BOSCH SECURITY SYSTEMS may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

3. COPYRIGHT. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT, are owned by BOSCH SECURITY SYSTEMS or its suppliers. The SOFTWARE PRODUCT is protected by the copyright laws and international treaty provisions. You may not copy printed materials accompanying the SOFTWARE PRODUCT.

   LIMITED WARRANTY - BOSCH SECURITY SYSTEMS warrants that (a) Access Easy Master Controller™ Software and (b) Access Easy Master Controller™ Access Control Panels and all input/output modules manufactured only by BOSCH SECURITY SYSTEMS will perform adequately in accordance with the accompanying User's Manual; and will be free from defects in materials and workmanship under its intended normal use and service for a period of 1 year from date of purchase.

   CUSTOMER REMEDIES - BOSCH SECURITY SYSTEMS'S entire liability and your exclusive remedy shall be, at BOSCH SECURITY SYSTEMS'S option, either (a) return of the price paid or (b) repair or replacement of the hardware or software that does not meet BOSCH SECURITY SYSTEMS'S limited warranty and which is returned to BOSCH SECURITY SYSTEMS with a copy of your purchase receipt. This limited warranty becomes void if failure of the hardware or software has resulted from abuse, accident or misapplication.

   NO LIABILITY OR CONSEQUENTIAL DAMAGES - Under no circumstances shall BOSCH SECURITY SYSTEMS or its suppliers be liable for any other damages whatsoever (including, without limitation, damages for business interruption, loss of business profits or other pecuniary loss) arising out of the use of or inability to use this BOSCH SECURITY SYSTEMS product. BOSCH SECURITY SYSTEMS total liability under any provision of this agreement shall be limited to the amount actually paid by you for the product.

Table of Contents

1	**Before You Begin**	**11**
2	**Introduction to Access Easy Master**	**12**
2.1	Features of Access Easy Master	12
2.2	Terms and Conventions	13
2.3	In addition to these terms, the following conventions are used:	13
3	**Logging In And Understanding Access Easy Master Main Menu**	**14**
3.1	Logging Into Access Easy Master	14
3.2	Main Menu Items	17
3.2.1	Activity	17
3.2.2	Manual Control	18
3.2.3	Card Database	18
3.2.4	System Admin	18
3.2.5	Panels Admin	19
3.3	Usage of the Buttons	20
4	**Activity**	**22**
4.1	View Activity	22
4.1.1	How To View Activity	23
4.1.2	How to Process Alarms/Events	26
5	**Manual Control**	**28**
5.1	Door Control	28
5.1.1	How to Unlock Reader Controlled Door	30
5.1.2	How to Lock Reader Controlled Door	31
5.1.3	How to Momentarily Unlock Reader Controlled Door	32
5.2	Input Control	33
5.2.1	How to Arm/Disarm an Input Point	36
5.2.2	How to Arm an Alarm Zone	36
5.3	Output Control	37
5.3.1	How to Turn On/Off Output Points	40
6	**Card Assignment**	**41**
6.1	The Card Parameters	42
6.1.1	Card Details	42
6.2	Adding and Deleting Cards	47
6.2.1	How to Add a New Card	47
6.2.2	How to Add a Batch of Cards	48
6.2.3	How to Delete a Batch of Cards	51
6.3	How to Import and Export Card Database	51
6.3.1	How to Export the Card Database	51
6.3.2	How to Import the Card Database	56
6.3.3	Cards Enrolment Operation	57
6.3.4	Card Enrolment of Card with Unknown Wiegand Format	57

6.4	How to Use Search Function	61
6.5	How to Generate Card Assignment Report	62
7	**Access Levels**	**65**
7.1	The Access Levels page	65
7.2	How to Configure Access Levels	66
7.3	How to Print Access Level Report	67
8	**Users Setup**	**68**
8.1	Setting User Access	68
8.1.1	How to Change User Name and Password	69
8.1.2	How to Change the Access to Menu Items	70
9	**Panel Setup**	**71**
9.1	How to Add an Access Easy Controller	71
9.1.1	How to download database to controller	72
9.2	How to download database to Panel	73
10	**Holidays**	**75**
10.1	How to configure Holidays	76
10.2	How to Generate a Holidays Report	77
11	**Schedules**	**79**
11.1	System Behaviour when using Schedule	80
11.2	How to Configure Schedules	81
11.3	How to Generate a Schedule Report	83
12	**Server Setup**	**85**
12.1	Network Settings	85
12.1.1	How to Edit Network Settings	86
12.2	Auto Logout Timer	86
12.2.1	How to set the Auto Logout Timer	86
12.3	Card Format	86
12.3.1	How to Configure New Card Format	87
12.4	View Activity Setting	90
12.4.1	How to Edit View Activity Setting	90
12.5	Company Profile	90
12.5.1	How to Edit Company Profile	91
12.5.2	How to Edit the Department List	91
12.6	Set Date & Time	93
12.6.1	How to Set the Date & Time	93
12.7	Default Settings	95
12.7.1	How to Edit the User Definable Fields	95
12.7.2	How to Edit the Facility Code	96
12.7.3	How to Edit the Date Format	96
12.7.4	How to Edit the Time Format	96
12.8	Housekeeping	96

12.8.1 How to Use the Manual Housekeep 97
12.8.2 How to Use the Auto Housekeep 97
12.9 Alarm Event Setup 97
12.9.1 Alarm Priority Setup 99
12.9.2 Alarm Event Condition Setup 101
12.9.3 Alarm Instruction Message setup 105

13 Report Generation 106
13.1 How to Set Criteria for Report Generation 106
13.2 How to Save Criteria for Future Use 113
13.3 How to Generate Report Using Saved Criteria 114
13.4 How To Generate Audit Log Report 115
13.4.1 User Log 115
13.4.2 System Log 116

14 Database Backup 118
14.1 How to Perform Database Backup 118
14.2 How To Restore System Database 120

15 Reboot, Shutdown and Logout 121
15.1 Reboot Function 121
15.2 Shutdown Function 122
15.3 Logout Function 122

16 Panels Admin 123
16.1 How To Choose Individual Panel To Admin 123
16.2 How to Setup Access Groups 124
16.2.1 How to Configure/Edit Access Group parameters 125
16.2.2 How to Generate a Print Preview of the Access Groups Report 126
16.3 How to Setup Card Readers 127
16.3.1 Reader Function 128
16.3.2 Reader Options 130
16.3.3 Scheduling Options 132
16.3.4 Door Output Settings (For Entry Reader, Entry and Arm/Disarm Reader) 134
16.3.5 Door Input Settings (For Entry Reader, Entry and Arm/Disarm Reader) 135
16.3.6 Floor Output Settings (For Elevator Reader Only) 137
16.3.7 PIN Code Settings 138
16.3.8 Anti-Passback (APB) Settings 140
16.3.9 Dual Card Configuration 143
16.3.10 How to generate a Print Preview of the Card Reader Report 144
16.4 Input Setup 145
16.4.1 Alarm Zone Description 148
16.4.2 How to generate a Print Preview of the Input Point Report 149
16.5 Output Setup 150
16.5.1 How to Generate a Print Preview of the Output Point Report 152
16.6 Advance I/O Setup 153
16.6.1 Guard Tour 153
16.6.2 Feed Through 154

16.6.3 OR Logic 155
16.6.4 AND Logic 156
16.6.5 XOR Logic 156
16.6.6 NAND Logic 157
16.6.7 Interlock / Man Trap 158
16.6.8 Up-Down Counter 162
16.6.9 Exit Door 163
16.6.10 One Shot 165
16.7 Input Point Configuration 166
16.7.1 To activate Input Point Configuration 166
16.7.2 To Select 2 State Non-Supervised, 2 State Supervised or 4 State Supervised 167
16.8 Email/SMS Configuration 168
16.8.1 Send To 169
16.8.2 Message field 170
16.8.3 Devices 170
16.8.4 Cardholders 171
16.8.5 Events 172
16.8.6 Lateness Report 173
16.8.7 Email Server Settings 176
16.8.8 SMS Server Settings 177
16.9 Reset APB 180
16.9.1 How To Reset APB by Card Number wrt Reader / All Readers 180
16.9.2 How to reset APB based on Name wrt Reader / All Readers 181
16.9.3 How to reset APB by All Card numbers wrt Reader / All Readers 181

17 How to Configure the Access Easy Master IP Address 182
17.1 For PC Users 182
17.1.1 Changing the PC's IP address 182
17.1.2 Settings to be made to the Web browser 186
17.1.3 Changing the IP address of Access Easy Master 189
17.2 For Macintosh Users 190
17.2.1 Changing the Macintosh's IP address 190
17.2.2 Settings to be made to the Web browser 191

18 Accessing and Understanding Access Easy for Master Main Menu 194
18.1 Connecting to Access Easy for Master 194
18.2 Logging onto Access Easy for Master 194
18.2.1 Logging onto Access Easy for Master 195
18.2.2 Logging off from Access Easy for Master 195
18.3 Understanding the Home Page Main Menu Groups 196
18.3.1 Manual Control 197
18.3.2 Panel Admin 197
18.3.3 Panel Maintenance 197
18.3.4 Logout 197
18.4 Navigating Through Access Easy for Master page 198

19 Door Control 200
19.1 To activate Door Control 201
19.1.1 To control the Doors manually 202

20	**Input Control**	**203**
20.1	To activate Input Control	204
20.1.1	To control (Arm/Disarm) an Input Point	206
20.1.2	To control (Arm/Disarm) the Alarm Zone	207
21	**Output Control**	**208**
21.1	To activate Output Control	209
21.1.1	To control the Output Points	210
22	**Reset APB**	**211**
22.1	To activate Reset APB	211
22.1.1	To reset APB based on Card Number wrt Reader / All Readers	211
22.1.2	To reset APB based on Name wrt Reader / All Readers	212
22.1.3	To reset APB by All Card numbers wrt Reader / All Readers	213
22.2	To generate a Print Preview of the report	213
22.2.1	To generate APB Zones Report	213
23	**Panel Setup**	**215**
23.1	To activate Panel Setup	215
23.2	Network Setting	216
23.2.1	To Configure LAN 1 Network Setting	216
23.3	Remote PC Addresses	217
23.3.1	To edit Remote PC Addresses	217
23.4	Email Server Setup Information	217
23.4.1	To Configure the Email Server Setup Information	218
23.5	Dial In IP Setup Information	218
23.5.1	To edit the Dial In IP Settings Information	219
23.5.2	Access Easy Master IP Address Settings for Access Easy for Master	219
23.5.3	SMS Server Settings Information	220
23.6	Set Date & Time	224
23.6.1	To activate Date & Time Setting	224
23.6.2	To set the Date & Time	224
23.7	Auto Logout Timer	225
23.7.1	To activate Auto Logout Timer	225
23.8	Audit Log	225
23.8.1	To View the User Log	226
23.8.2	To View System Log	227
24	**Users**	**229**
24.1	To activate Users	229
24.1.1	To edit User ID and Password	229
25	**Dial in User**	**230**
25.1	Setting up Windows for Dial-in	230
25.2	Setting up Macintosh for Dial-in	236

26	**Update Flash**	**240**
26.1	To activate Update Flash	241
26.1.1	To Update Panel Software	242
27	**Reboot Panel**	**243**
27.1	To activate Reboot Panel	243
28	**APPENDIX A Selecting Events, Devices and Cardholders for Report Generation**	**244**
29	**APPENDIX B Configuring Alarm Events**	**246**
30	**APPENDIX C Activity Transactions**	**247**
30.1	Alarm Activity	247
30.2	Restore Activity	247
30.3	Valid Activity	248
30.4	Time Attendance	248
31	**APPENDIX D Email/SMS Configuration Table**	**249**
32	**APPENDIX E Setting up a Timeserver (Windows 2000 and XP Professional)**	**252**
32.1	For Windows 2000	252
32.2	For Windows XP Professional	256
33	**APPENDIX F Initial Setup To Access Easy Controller**	**263**
33.1	Procedure to set the IP Address of computer	264
33.1.1	For PC Users	264
33.2	For Macintosh Users	268
33.3	Setting to be made to the Web browser	270
33.3.1	For PC User	270
33.4	For Macintosh Users	273
33.5	Setting the Access Easy Controller IP Address Through Address Resolution Protocol (ARP)	276
34	**APPENDIX G**	**279**
34.1	Preparing the WAVECOM GSM Modem for Access Easy Controller	279
34.2	How to test the GSM modem	281

1 Before You Begin

The Access Easy Master Software User Manual contains two detailed software setup information, they are

- Access Easy Master Controller Software.
- Access Easy for Master Controller Software.

Access Easy Master Software is the main software that administers and controls all Access Easy Controllers whereas Access Easy for Master Software only supports minimal functions on its respective Access Easy Controller.

In this manual, we will use the following terminologies to describe the following software.

Name	Terminology
Access Easy Master Controller Software	Access Easy Master
Access Easy For Master Controller Software	Access Easy For Master
Access Easy Controller Hardware	Access Easy Controller

This manual will describe the Access Easy Master Controller Software from Chapter 2 to 17 whereas Chapter 18 to 27 will describe the Access Easy for Master Controller Software.

2 Introduction to Access Easy Master

Access Easy Master is a revolutionary invention that takes advantage of the web technology age by changing the way an electronic access control system is implemented.

The conventional way of implementing a typical access control system requires installation of application programs that are used to remote control and monitor a controller in the system. Furthermore, application programs that are designed for a specific operating system have to be re-developed before it can run on another operating system.

Access Easy Master uniquely combines the features of Web technologies and Access Control functionality into one complete unit. Such powerful combination provides a highly cost-effective solution, which truly offers to user the simplicity and ease-of-use associated with the popular Web interface while incorporating a rich suite of sophisticated security features essential for small to medium-sized businesses.

The design of Access Easy Master adopts the common desktop metaphor for all Windows applications for consistency and ease of use. The same "look-and-feel" such as buttons and check boxes that you have experienced in other Windows applications will be seen in Access Easy Master.

The unique feature in Access Easy Master is, all the Access Easy Controller can be centrally administered from a single Access Easy Master.

2.1 Features of Access Easy Master

- Cross-operating platform/system interoperability. Whether it is a PC, Mac or Unix machine, Access Easy Master gives you complete flexibility of operating on these platforms without any extra effort in setting up.
- Easy to install as Access Easy Master adopts the 'Plug n Play' concept. Simply connect a network cable from the Access Easy Master to a network hub, follow by running a web browser program to set up the Access Easy Master and the system will be up and running in no time.
- Easy to operate for end users as it uses the intuitive web interface that makes controlling or monitoring the system like performing Net surfing! This also implies that minimum training is needed for installers, distributors and end users.
- Easy to access Access Easy Master from any computer (or client) that exists in your network, be it in a LAN or WAN configuration! No longer are users required to have a dedicated computer to handle the controller as any computer can now be used to access the Access Easy Master. Such powerful feature allows users to save costs by fully optimising their existing resources and cutting down on any unnecessary spending on new hardware.
- Easy to maintain or upgrade the system as it is not dependent on any operating platform/system to run on. Upgrading the Access Easy Master does not require users to upgrade their computers and operating systems. Likewise, upgrading the operating system e.g. from Win 95 to Win 98/NT/2000 will not affect the Access Easy Master system configuration. Such investment produces long term cost savings for the users.

- Time and cost savings in the installation, testing and commissioning of Access Easy Master as no application programs are required to be installed on central computer(s). This

implies greater profits at a shorter time for both distributors and installers.

The design of Access Easy Master adopts the common desktop metaphor for all Windows applications for consistency and ease of use. The same "look-and-feel" such as buttons and check boxes that you have experienced in other Windows applications will be seen in Access Easy Master.

2.2 Terms and Conventions

If you are a Microsoft Windows user, the terms in this User's Manual should be familiar to you. If you have not used Windows before, or would like a refresher course, please read this section to become familiar with some common terms.

- *Pointer* refers to the arrow-shaped cursor on the screen.
- *Choose* means to move the pointer to a menu, command, tool, or button and press the left mouse button. This term is synonymous with *click*.
- *Select* means to mark an item with the selection cursor, which can appear as a highlight, a dotted rectangle, or both.
- *Double-click* means to press the left mouse button twice rapidly.
- *Drag* means to hold down the left mouse button, move the pointer to another location on the screen, and release the mouse button.
- *Field* is a category of information. It could be card numbers, names, shift codes or dates.

2.3 In addition to these terms, the following conventions are used:

- Menu, command, table names are shown in *italic* type.
- Word in Bold represents the key on the keyboard. For example, Alt indicates the Alt key in the keyboard.
- When two keys are used together to perform a task, they are separated with a plus sign.

For example, the key combination Ctrl + F4 means you hold down the Ctrl key and press the F4 key.

3 Logging In And Understanding Access Easy Master Main Menu

Before the user starts to understand Access Easy Master main menu, let us take a look at the procedures in logging in first.

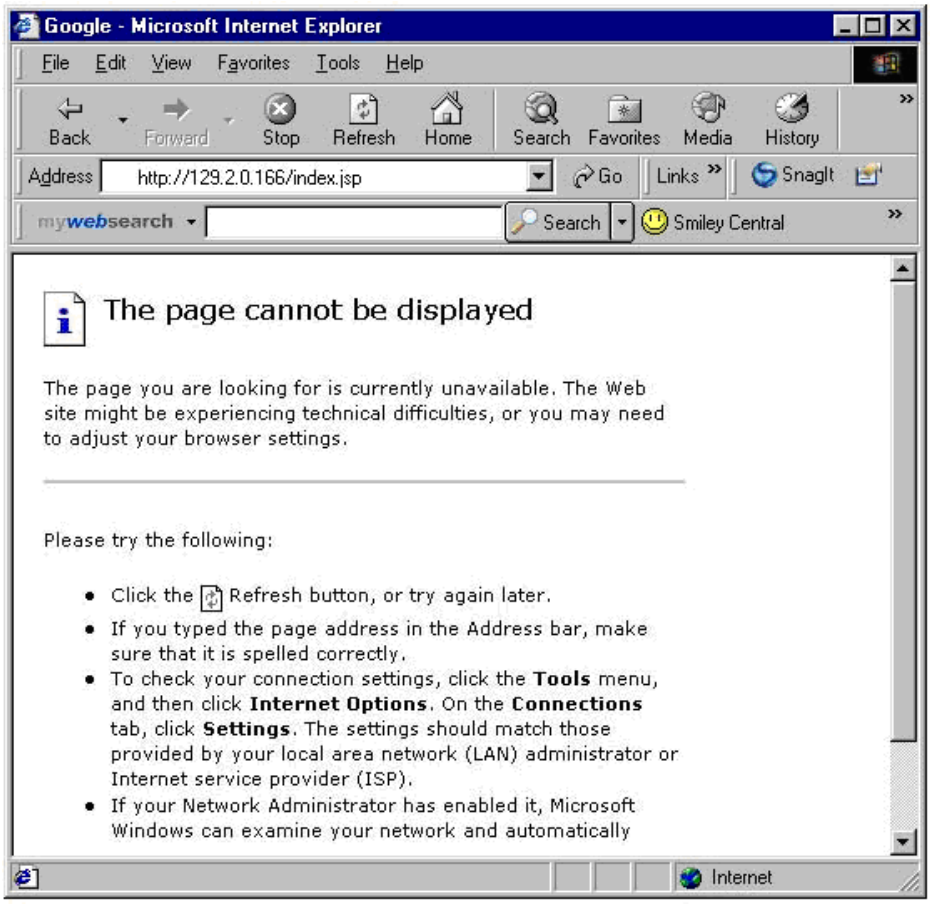
3.1 Logging Into Access Easy Master

In order to login to Access Easy Master, a computer with a standard web browser program such as Internet Explorer version 6.0 and above, or Netscape version 7.0 and above, is required on the computer.

1. To get connected to Access Easy Master, run your web browser page with the default URL address for the Access Easy Master.

Enter URL address for Access Easy Master
iVision - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History
Address 129.2.0.166
Go Links SnagIt

2. If the page cannot be displayed, as shown below, follow steps 3 to 8. If the *Security Alert box* appears, follow steps 7 to 8.

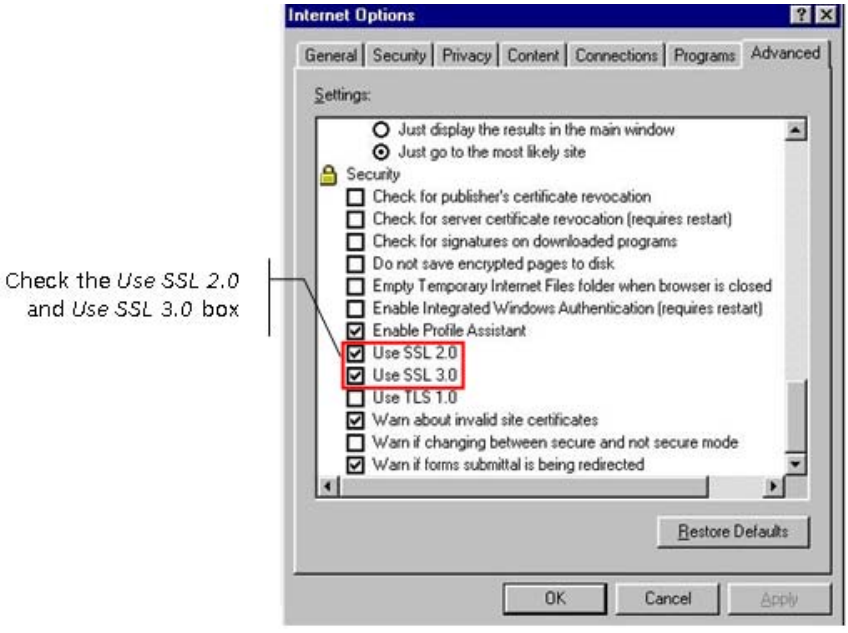

Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History
Address http://129.2.0.166/index.jsp
Go Links SnagIt
mywebsearch Search Smiley Central
The page cannot be displayed
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.
Please try the following:
Click the Refresh button, or try again later.
If you typed the page address in the Address bar, make sure that it is spelled correctly.
To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
If your Network Administrator has enabled it, Microsoft Windows can examine your network and automatically
Internet

3. Go to the menu items of the web browser and select *Tools, Internet Options*.

4. A I*nternet Options* window will appear as shown below. Select *Advanced*.

Select Advanced
Internet Options
General Security Privacy Content Connections Programs Advanced
Home page
You can change which page to use for your home page.
Address: 129.2.0.166
Use Current Use Default Use Blank
Temporary Internet files
Pages you view on the Internet are stored in a special folder for quick viewing later.
Delete Cookies... Delete Files... Settings...
History
The History folder contains links to pages you've visited, for quick access to recently viewed pages.
Days to keep pages in history: 0 Clear History
Colors... Fonts... Languages... Accessibility...
OK Cancel Apply

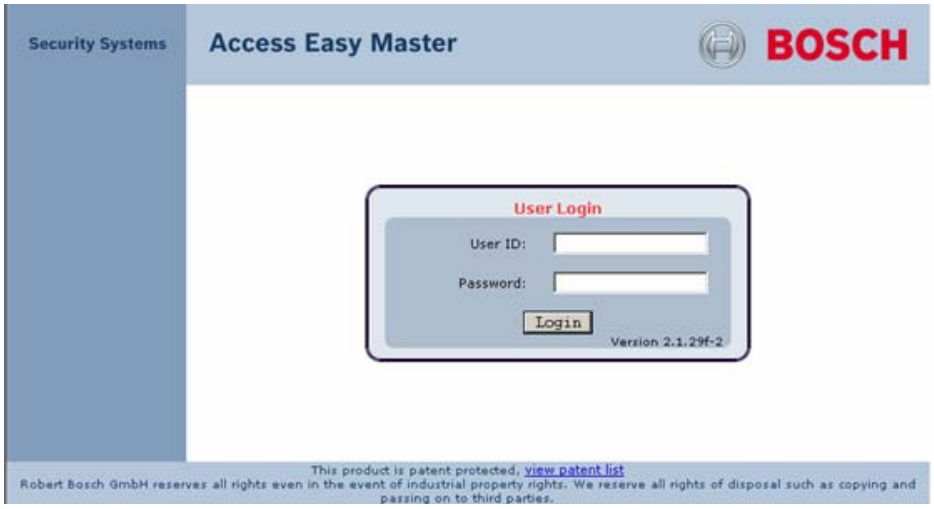
5. A screen as shown below appears. Check the *Use SSL2.0* and *Use SSL 3.0* box.


Check the Use SSL 2.0 and Use SSL 3.0 box
Internet Options
General Security Privacy Content Connections Programs Advanced
Settings:
Just display the results in the main window
Just go to the most likely site
Security
Check for publisher's certificate revocation
Check for server certificate revocation (requires restart)
Check for signatures on downloaded programs
Do not save encrypted pages to disk
Empty Temporary Internet Files folder when browser is closed
Enable Integrated Windows Authentication (requires restart)
Enable Profile Assistant
Use SSL 2.0
Use SSL 3.0
Use TLS 1.0
Warn about invalid site certificates
Warn if changing between secure and not secure mode
Warn if forms submittal is being redirected
Restore Defaults
OK Cancel Apply

6. Click on [OK] and go to the menu items of the web browser and select *View, Refresh*. The *Security Alert* box appears on the screen.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

7. Click [Yes] to proceed and the User Login page appears. If [No] is selected, the page remains blank and the user will not be able to see the *User Login* page. To proceed, go to the menu items of the web browser and select *View, Refresh*. The *Security Alert* box will appear again. Click [Yes] to proceed.


Security Systems
Access Easy Master
BOSCH
User Login
User ID:
Password:
Login
Version 2.1.29f-2
This product is patent protected. view patent list
Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

8. Enter your assigned User ID and Password. Click on the [Login] button to login.

Upon successful login to the Access Easy Master, the user will see the View Activity page in Alarm transactions. It is the default page whenever the user logins to Access Easy Master.

NOTICE!
The default User ID is iuser1 and the default Password is 8088.

Security Systems
Access Easy Master
BOSCH
Alarm Valid Restore All Time Attendance
View Activity
Activity
View Activity
Manual Control
Door Control
Input Control
Output Control
Card Database
Card Assignment
Access Levels
System Admin
Users Setup
Panel Setup
Holidays
Schedules
Server Setup
Report Generation
Database Backup
Reboot
Shutdown
Logout
Panels Admin
172.16.10.92
Access Groups
Card Readers
Input Setup
Output Setup
Advance I/O Setup
Input Point Configuration
Email/SMS Configuration
Reset APB
Alarm Activities
Panel No | Date | Location | Activity Description
Priority | Time | Card No | User Name
20 (2) | 23 Dec 2005 11:40:41 | Reader 2 10 | Access Denied - Passback Card Number:10
1 (1) | 23 Dec 2005 11:40:39 | Reader 3 (0)31 | Invalid Card Standard 26 bit Format
20 (2) | 23 Dec 2005 11:40:37 | Reader 1 9 | Invalid Second Card Read Card Number:9
1 (1) | 23 Dec 2005 11:40:36 | Reader 2 (0)30 | Invalid Card Standard 26 bit Format
20 (2) | 23 Dec 2005 11:40:34 | Reader 4 8 | Exit Denied - Passback Card Number:8
1 (2) | 23 Dec 2005 11:40:33 | Reader 1 29 | Invalid First Card Read Card Number:29
20 (1) | 23 Dec 2005 11:40:09 | Reader 4 (0)32 | Invalid Card Standard 26 bit Format
20 (1) | 23 Dec 2005 11:40:06 | Reader 3 (0)31 | Invalid Card Standard 26 bit Format
20 (1) | 23 Dec 2005 11:40:03 | Reader 2 (0)30 | Invalid Card Standard 26 bit Format
1 (1) | 23 Dec 2005 11:39:01 | Reader 4 (0)32 | Invalid Card Standard 26 bit Format
Left Pane
The left pane displays the main menu items for ease of operation. Those in bright yellow background are the Panel's menu group.
Right Pane
The right pane displays the work area of the menu items selected.

The pages will have the main menu items on the Left Pane and the work area on the Right Pane. This presentation is standard throughout the entire Access Easy Master's pages.

3.2 Main Menu Items

The main menu items are shown on the Left Pane of each page. Below explains each Access Easy Master main menu item in brief.

3.2.1 Activity

Activity allows the user to view the activities that have taken place in the system. The sub menu items of *Activity* is *View Activity*.

View Activity

View Activity shows transactions generated due to access control, system control, and alarm conditions. The transactions are categorised into the following: Alarm, Valid, Restore and Time Attendance. User can view only a specific category as mentioned above or All Transactions.

Using Java Applet technique, all the activities and status on the *Manual Control* pages (Door Control, Input Control and Output Control) will be automatically updated in real time.

3.2.2 Manual Control

Manual Control allows the user to control the door, input points and output points manually by having priority over the control set by the system. The sub menu items of *Manual Control* are *Door Control*, *Input Control* and *Output Control*.

Door Control

Door Control allows the user to check the status of all the doors and send a command to either momentarily unlock or permanently unlock / lock the door without having to be at the door location.

Input Control

Input Control allows the user to check the status of all the input points assigned to specific alarm zones and to send a command to arm / disarm the zone manually.

Output Control

Output Control allows the user to check the status of all the output points and send a command to turn on / off the points manually.

3.2.3 Card Database

Card Database allows the user to administer the card details, functionality and the access levels of the card. The sub menu items of *Card Database* are *Card Assignment* and *Access Levels*.

Card Assignment

Card Assignment allows the administrator to assign cards to users. The Access Level for the user and the Card Functionality is configured in this section also.

Access Levels

Access Levels allows the user to define Access Groups belonging to different Access Easy Controller into groups. These groups when assigned to a cardholder allow him to access to doors over multiple Access Easy Controller, hence enabling the administrator to manage cardholders' access in a centralized location.

3.2.4 System Admin

System Admin menu allows the user to setup the different aspects of the system such as the users, controller and server side. It also allows the user to generate reports from the system and backup database of the system. The sub menu items of *System Admin* are *Users Setup*, *Panel Setup, Holidays, Schedules, Server Setup, Report Generation, Database Backup,* Reboot, *Shutdown* and *Logout*.

Users Setup

Users Setup allows the user to set-up the User ID and Password including access rights to the various menu items.

Panel Setup

Panel Setup allows the user to admit Access Easy Controller to join the system network.

Holidays

Holidays allows the user to setup centralized Holiday dates that are applicable to all the Access Easy Controller.

Schedules

Schedules allow the user to setup centralized Schedules available to all the Access Easy Controller that can be assigned to schedules of Readers, or to Access Groups.

Server Setup
Server Setup allows the user to configure the following settings:

Network Settings	Set Date and Time
Auto Logout Timer	Default Settings
Card Format	Housekeeping
View Activity Setting	Alarm Event Setup
Company Profile	

Report Generation
Report Generation allows the user to generate activity reports for particular date/s and time based on Devices, Cardholders and Events.

Database Backup
Database Backup allows the user to save a backup of the database to the local hard disk and also allows the user to restore the database in the event of any controller failure.

Reboot
Reboot allows the user to reboot the Access Easy Master from remote without having to be at the Access Easy Master itself.

Shutdown
Shutdown allows the user to shutdown the system from remote without having to be at the Access Easy Master itself.

Logout
Logout allows the user to do a proper exit from the Access Easy Master.

3.2.5 Panels Admin

Panels Admin menu allows the user to administer the individual Access Easy Controller. The sub menu items of *Panels Admin* are *Access Groups, Card Readers, Input Setup, Output Setup, Advance I/O Setup, Input Point Configuration, Email/SMS Configuration* and *Reset APB*.

Access Groups
Access Groups allow the user to define a list of Readers, which the cardholders can access within certain authorised time periods (pre-defined Schedule).

Card Readers
Card Readers are used to define the function of the Readers and their parameters, such as door settings, etc.

Input Setup
Input Setup is used to set-up Alarm Monitoring Point to be armed/disarmed based on Schedule or via an assigned Reader. It also allows the definition of which output points to trigger should an alarm be detected.

Output Setup
Output Setup is used to set up the triggering of output relay based on Schedules. For example, this can be used to turn on lighting in an area after office hours.

Advance I/O Setup
Advance I/O Setup enables the rerouting of physical or logical information from one operation to another. Due to its flexibility, the type of operation it can achieve is dependent on the installer.

Input Point Configuration

Input Point Configuration allows the user to invert the logical state of the input that is seen by the Access Easy Controller, as well as to select the monitoring state of the Input Point.

Email/SMS Configuration

Email/SMS Configuration allows the user to setup the Email and SMS Server Settings, to allow the Access Easy Controller to send out messages or email to selected mobile numbers or email addresses according to the selected Devices, Cardholders and Events. Lateness Report can also to sent to configured email addresses.

Reset APB

Reset APB allows the user to reset the Anti-Passback (APB) feature once it is violated.

3.3 Usage of the Buttons

Another important part to understand is the meaning of the buttons. The buttons that appear at the bottom of each screen can be explained as follows:

Button	Description
	The save button saves the current settings to the (Dynamic RAM) DRAM and refreshes the current web page.
	The add button provides the following functions: - ▶ It carries out the addition process during a batch card operation. ▶ It also adds a selected parameter to a list window.
	The delete button provides the following functions: - ▶ It deletes all configurable parameters and set it to default. ▶ It also removes a selected parameter from the list window.
	The next button provides the following functions: - ▶ It saves the setting made on the current screen and ▶ It brings up the next screen.
	The list button provides a few function: - ▶ It allows you to go back to the first web page of a menu item. ▶ It can also be use in place of the cancel button to abort changes. However, condition applies that none of the other buttons namely, the next, prev or save is clicked prior to this. ▶ In report generation, the list button is used to obtain a print preview of the report.

Button	Description
	The previous button has similar function as the next button, ▶ It saves the setting made on the current screen and ▶ It brings up the previous screen.
	The reset button provides the following functions: - ▶ It is use to reset APB violation. ▶ It is use to clear the field in the Holiday date setting.
	The cancel button abort changes and revert to previously saved settings.

4 Activity

Each activity transaction such as Door Forced Open, Door Held Open, etc. is captured by Access Easy Master and displayed on the *View Activity* web page in real-time mode according to the transaction occurrence date and time.

The activity transactions are categorised into 4 groups. They are: -

- Alarm Activity,
- Valid Activity,
- Restore Activity, and
- Time Attendance.

Please refer to *Appendix C Activity Transactions* for the activity transactions in the different groups.

4.1 View Activity

On the web page, user is given the option to view one of the following: -

- Alarm Transactions,
- Valid and Alarm Transactions,
- Restore and Alarm Transactions,
- Time Attendance, or
- All Transactions.

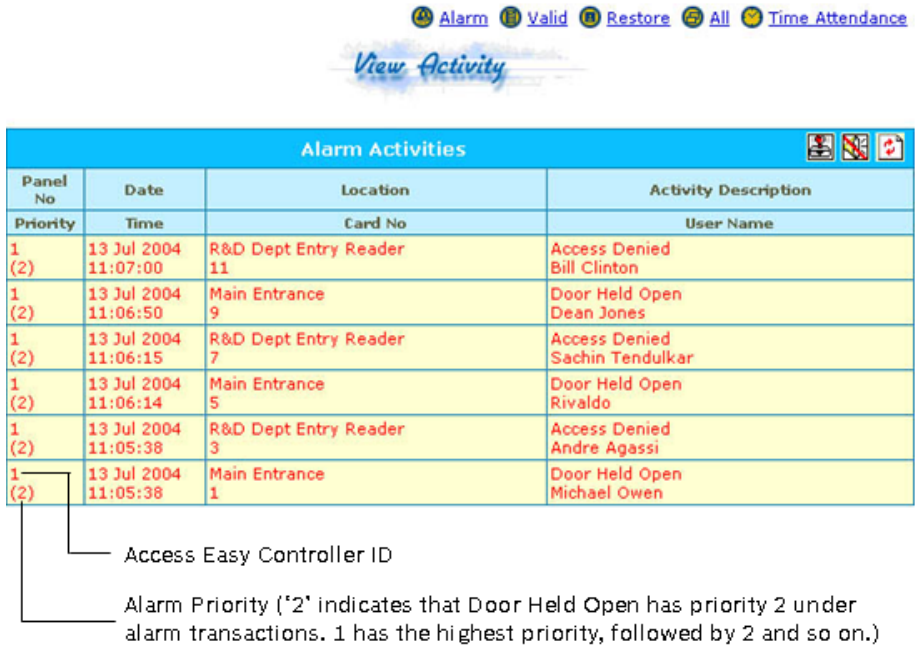
The number of records to view on screen is configurable by the user, up to a maximum of 70 records (see NOTICE). Please refer to *Chapter 12 Server Setup, View Activity Setting* for details on setting the number of transaction records to view on screen.

NOTICE!
The *View Activity* web page is dynamic and will expand beyond the *"Number of Transactions To view"* setting to always accommodate transactions, up to 70 records, starting from the first "not acknowledged" alarm transaction up to the latest transaction.

When any of the alarm activity transactions is transacted, an alerting audio tone is sent to the PC. Please ensure that the PC's audio system is in working order and the volume is set to a reasonable level.

4.1.1 How To View Activity

Upon login to the Access Easy Master, the View Activity page for Alarm transactions will be displayed. However, at any other page you could select View Activity from the Left Pane to view the activities.


Alarm
Valid
Restore
All
Time Attendance
View Activity
Alarm Activities
Panel No
Date
Location
Activity Description
Priority
Time
Card No
User Name
1 (2) 13 Jul 2004 11:07:00 R&D Dept Entry Reader 11 Access Denied Bill Clinton
1 (2) 13 Jul 2004 11:06:50 Main Entrance 9 Door Held Open Dean Jones
1 (2) 13 Jul 2004 11:06:15 R&D Dept Entry Reader 7 Access Denied Sachin Tendulkar
1 (2) 13 Jul 2004 11:06:14 Main Entrance 5 Door Held Open Rivaldo
1 (2) 13 Jul 2004 11:05:38 R&D Dept Entry Reader 3 Access Denied Andre Agassi
1 (2) 13 Jul 2004 11:05:38 Main Entrance 1 Door Held Open Michael Owen
Access Easy Controller ID
Alarm Priority ('2' indicates that Door Held Open has priority 2 under alarm transactions. 1 has the highest priority, followed by 2 and so on.)

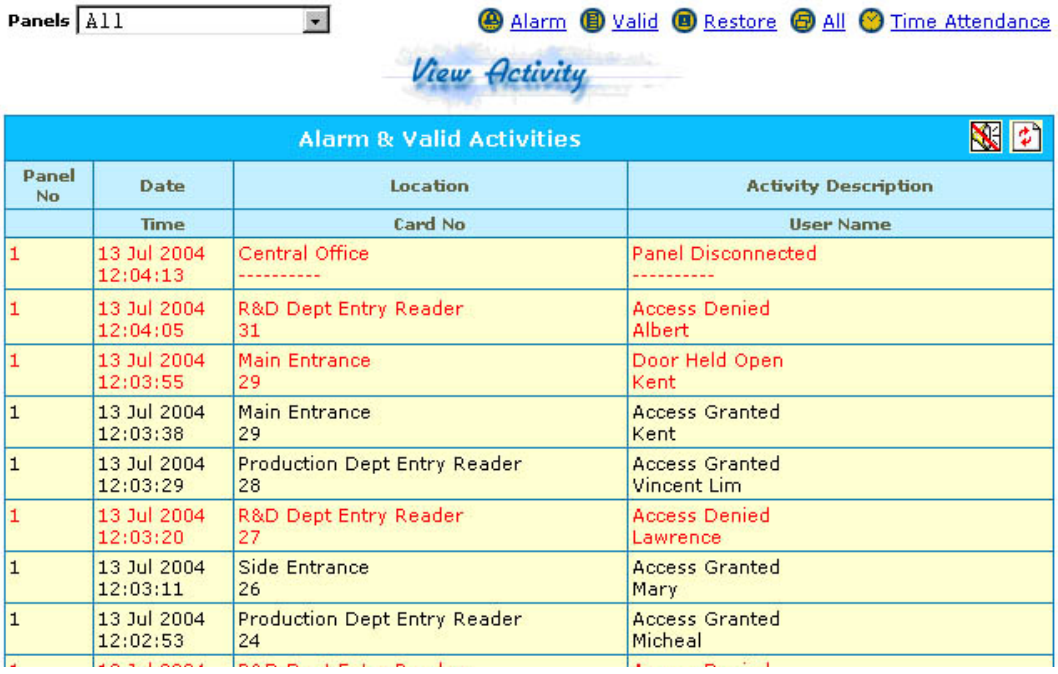
NOTICE!

The transactions are sorted by the alarm priority and date/time. Alarms having the highest priority are shown on the top of the list. Those alarms having the same priority will be sorted again by the date/time. Hence, the newest and highest priority alarm will always be shown on the top of the list. Please refer to *Chapter 12 Server Setup, Alarm Event Setup, Alarm Priority Setup* for more details.

These are some of the view activity menu items explained in brief.

Options	Description
Alarm	To display only Alarm transactions.
Valid	To display Valid and Alarm transactions.
Restore	To display Restored and Alarm transactions.
All	To display All transactions.
Time Attendance	To display only Time Clocking transactions.
	To acknowledge Alarm transactions.
	This will silence the audible tones on the Access Easy For Master.
	This will enable the audible tones on Access Easy For Master.
Panels All	To select a Access Easy Controller for which the user wants to view the activity only. We can view the activity for all the controllers or for selected controllers. This list box will not be available in the Alarm View.

1. Login to Access Easy Master and the *View Activity* screen will appear. It shows the Alarm activities. This is the default page for *View Activity*.
2. To include Valid transactions on the *View Activity*, click Valid. The screen will refresh and show the Valid and Alarm activities.


Panels All
Alarm
Valid
Restore
All
Time Attendance
View Activity
Alarm & Valid Activities
Panel No
Date
Time
Location
Card No
Activity Description
User Name
1 13 Jul 2004 12:04:13 Central Office ---------- Panel Disconnected ----------
1 13 Jul 2004 12:04:05 R&D Dept Entry Reader 31 Access Denied Albert
1 13 Jul 2004 12:03:55 Main Entrance 29 Door Held Open Kent
1 13 Jul 2004 12:03:38 Main Entrance 29 Access Granted Kent
1 13 Jul 2004 12:03:29 Production Dept Entry Reader 28 Access Granted Vincent Lim
1 13 Jul 2004 12:03:20 R&D Dept Entry Reader 27 Access Denied Lawrence
1 13 Jul 2004 12:03:11 Side Entrance 26 Access Granted Mary
1 13 Jul 2004 12:02:53 Production Dept Entry Reader 24 Access Granted Micheal

3. To include Restored transactions on the View Activity, click Restore . The screen will refresh and show the Restored and Alarm activities.

Restore & Alarm Activities

Panel No	Date / Time	Location / Card No	Activity Description / User Name
1	13 Jul 2004 11:53:37	Side Entrance 11856	Door Held Open Card Number:11856
1	13 Jul 2004 11:50:37	Central Office ----------	Connected to Server ----------
1	13 Jul 2004 11:48:21	Central Office ----------	Disconnected from Server ----------
1	13 Jul 2004 11:50:36	Central Office ----------	Panel Connected ----------
1	13 Jul 2004 11:48:22	Central Office ----------	Panel Disconnected ----------
1	13 Jul 2004 11:41:22	Main Entrance1 ----------	Door Held Open ----------
1	13 Jul 2004 11:41:22	Side Entrance ----------	Door Held Open ----------
1	13 Jul 2004 11:39:30	Central Office ----------	Connected to Server ----------
1	13 Jul 2004 11:38:28	Central Office ----------	Disconnected from Server ----------

4. To show All activities, click All . The screen will refresh and show All the activities.

All Activities

Panel No	Date / Time	Location / Card No	Activity Description / User Name
1	13 Jul 2004 12:34:07	Side Entrance 18	Access Granted Denezel Washington
1	13 Jul 2004 12:33:58	Main Entrance 17	Access Granted Sadique
1	13 Jul 2004 12:33:40	Production Dept Entry Reader 16	Access Granted Gurmit Singh
1	13 Jul 2004 12:33:31	R&D Dept Entry Reader 15	Access Denied James Cameroon
1	13 Jul 2004 12:33:30	Main Entrance 13	Door Held Open Bastiqula
1	13 Jul 2004 12:33:22	Side Entrance 14	Access Granted Pete Sampras
1	13 Jul 2004 12:33:13	Main Entrance 13	Access Granted Bastiqula
1	13 Jul 2004 12:33:04	Production Dept Entry Reader 12	Access Granted William Sim
1	13 Jul 2004 12:32:55	R&D Dept Entry Reader 11	Access Denied Bill Clinton
1	13 Jul 2004 12:32:54	Main Entrance 9	Door Held Open Dean Jones

5. To show Time Attendance activities, click Time Attendance . The screen will refresh and show the Time Attendance activities.

Time Attendance			
Panel No	Date	Location	Activity Description
	Time	Card No	User Name
1	12 Jul 2004 14:42:45	Production Dept Entry Reader 16	Clock Out Gurmit Singh
1	12 Jul 2004 14:42:00	R&D Dept Entry Reader 11	Clock Out Bill Clinton
1	12 Jul 2004 14:41:06	Side Entrance 6	Clock Out Tiger Woods
1	12 Jul 2004 14:40:21	Main Entrance 1	Clock Out Michael Owen
1	12 Jul 2004 14:39:27	Production Dept Entry Reader 28	Clock In Vincent Lim
1	12 Jul 2004 14:38:33	R&D Dept Entry Reader 23	Clock In Eric Ho

4.1.2 How to Process Alarms/Events

The *View Activity* provides a easy colour scheme to differentiate between new transactions, new alarms and acknowledged alarms: -

- All new transactions have a yellow background. The new transactions will appear in the *View Activity* in real-time mode.

1	08 Sep 2003 09:16:43	Entrance 2 16	Access Granted Jerry Maguire

- All Alarm transactions have red coloured text wording while other transactions have black coloured text wording.

1 (2)	08 Sep 2003 09:23:49	Side Entrance 2	Door Held Open William Sim

- When the web page refreshes automatically, the yellow background is replaced with grey background, except for Alarm transactions, which remain unless the button is activated.

1	08 Sep 2003 09:27:30	Entrance 2 16	Access Granted Jerry Maguire

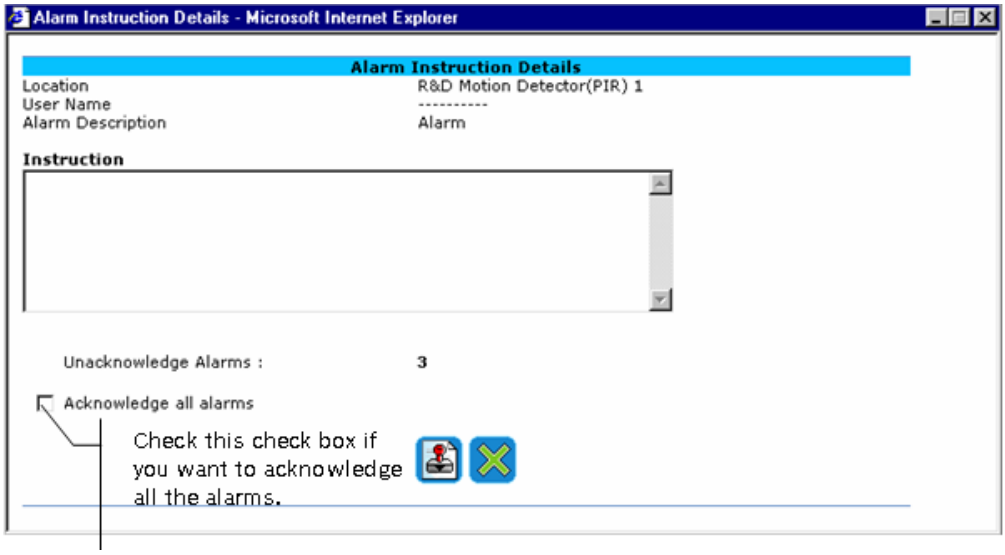
Process Event Transactions

New Valid and Restored transactions are shown in yellow background and black text. When the web page refreshes, the background will be changed to grey. Furthermore, depending on the View Activity Setting, the screen will be restricted to the number of transactions shown. However, unacknowledged alarms will still remain on the screen till they are acknowledged by the user.

Process Alarm Transactions

New alarms are shown in yellow background and red text. They will remain so till the user acknowledges the alarms. Refreshing the screen will not change the background to grey, as it will for Valid and Restore transactions.

User needs to acknowledge the alarm, by clicking on the button. This action will cause the *Alarm Instruction Details* window to pop up as shown below. However, this button is only shown when the View Activity page is in Alarm transactions. When viewing *Valid, Restore, All* or *Time Attendance* transactions, the button is not shown.



This window shows the alarm that you are acknowledging and the instruction message pre-configured in the system for this alarm.

NOTICE!
Access Easy Master allows the user to configure instruction messages to different alarms. These instruction messages can be configured in *Chapter 12 Server Setup, Alarm Event Setup, Alarm Instruction Message Setup* for details.

5 Manual Control

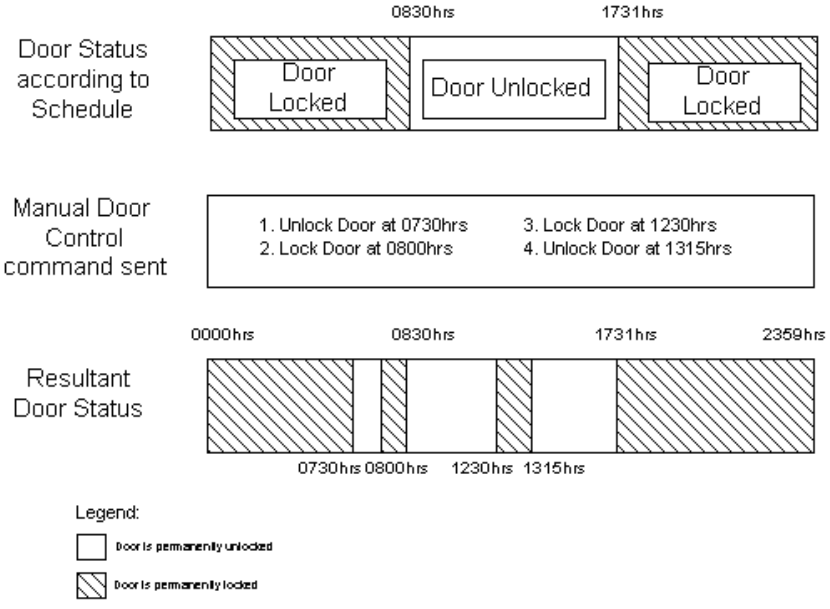
The *Manual Control* menu in Access Easy Master comprises of *Door Control, Input Control* and *Output Control*. Each control provides a means to easily modify and control any card reader, input or output point in the system. This chapter shall discuss each of the control in detail.

5.1 Door Control

Door Control allows the user to check the status of all the doors and send a command to either Momentarily Unlock or permanently Unlock/Lock the door from remote.

As this is a control operated by a user manually, it has priority over the control set by the system. However, the system will take over and resume normal operation once it encounters a valid Schedule Interval.

Here is an example to illustrate the condition.
The setting for Interval 1 is Start - 0830hrs and End - 1730hrs.
Interval 2,3, and 4 has no setting.



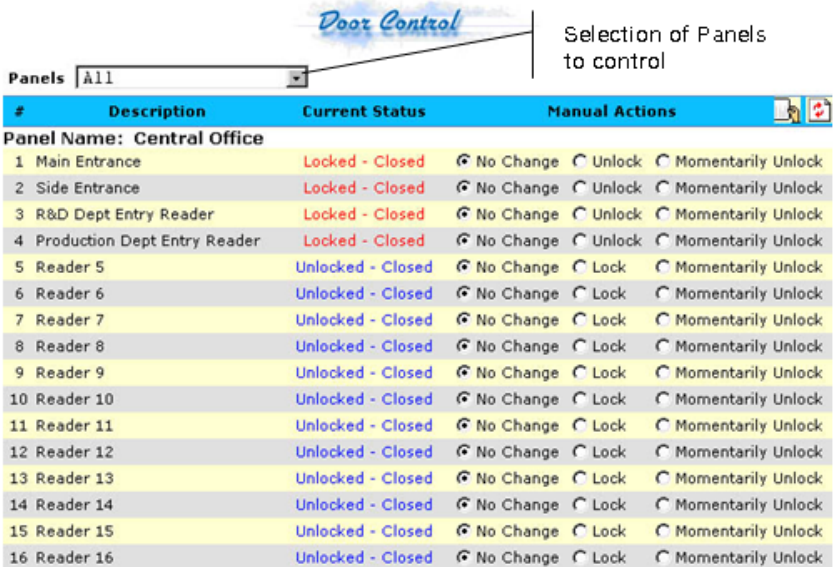
Notice that the system resumes normal operation as according to Schedule at 0830hrs and 1731hrs.

Now let us continue with *Door Control*.

1. From the Access Easy Master main menu page, click on *Door Control*.

Security Systems
Access Easy Master
BOSCH
Alarm Valid Restore All Time Attendance
View Activity
Activity
View Activity
Manual Control
Door Control
Input Control
Output Control
Card Database
Card Assignment
Access Levels
System Admin
Users Setup
Panel Setup
Holidays
Schedules
Server Setup
Report Generation
Database Backup
Reboot
Shutdown
Logout
Panels Admin
172.16.10.92
Access Groups
Card Readers
Input Setup
Output Setup
Advance I/O Setup
Input Point Configuration
Email/SMS Configuration
Reset APB
Alarm Activities
Panel No | Date | Location | Activity Description
Priority | Time | Card No | User Name
20 (2) | 23 Dec 2005 11:40:41 | Reader 2 | 10 | Access Denied - Passback | Card Number:10
1 (1) | 23 Dec 2005 11:40:39 | Reader 3 | (0)31 | Invalid Card | Standard 26 bit Format
20 (2) | 23 Dec 2005 11:40:37 | Reader 1 | 9 | Invalid Second Card Read | Card Number:9
1 (1) | 23 Dec 2005 11:40:36 | Reader 2 | (0)30 | Invalid Card | Standard 26 bit Format
20 (2) | 23 Dec 2005 11:40:34 | Reader 4 | 8 | Exit Denied - Passback | Card Number:8
1 (2) | 23 Dec 2005 11:40:33 | Reader 1 | 29 | Invalid First Card Read | Card Number:29
20 (1) | 23 Dec 2005 11:40:09 | Reader 4 | (0)32 | Invalid Card | Standard 26 bit Format
20 (1) | 23 Dec 2005 11:40:06 | Reader 3 | (0)31 | Invalid Card | Standard 26 bit Format
20 (1) | 23 Dec 2005 11:40:03 | Reader 2 | (0)30 | Invalid Card | Standard 26 bit Format
1 (1) | 23 Dec 2005 11:39:01 | Reader 4 | (0)32 | Invalid Card | Standard 26 bit Format

2. The *Door Control* screen will appear.


Door Control
Selection of Panels to control
Panels All
Description Current Status Manual Actions
Panel Name: Central Office
1 Main Entrance Locked - Closed No Change Unlock Momentarily Unlock
2 Side Entrance Locked - Closed No Change Unlock Momentarily Unlock
3 R&D Dept Entry Reader Locked - Closed No Change Unlock Momentarily Unlock
4 Production Dept Entry Reader Locked - Closed No Change Unlock Momentarily Unlock
5 Reader 5 Unlocked - Closed No Change Lock Momentarily Unlock
6 Reader 6 Unlocked - Closed No Change Lock Momentarily Unlock
7 Reader 7 Unlocked - Closed No Change Lock Momentarily Unlock
8 Reader 8 Unlocked - Closed No Change Lock Momentarily Unlock
9 Reader 9 Unlocked - Closed No Change Lock Momentarily Unlock
10 Reader 10 Unlocked - Closed No Change Lock Momentarily Unlock
11 Reader 11 Unlocked - Closed No Change Lock Momentarily Unlock
12 Reader 12 Unlocked - Closed No Change Lock Momentarily Unlock
13 Reader 13 Unlocked - Closed No Change Lock Momentarily Unlock
14 Reader 14 Unlocked - Closed No Change Lock Momentarily Unlock
15 Reader 15 Unlocked - Closed No Change Lock Momentarily Unlock
16 Reader 16 Unlocked - Closed No Change Lock Momentarily Unlock

Description provides the Controller Name and the Door Readers allocated to it.

Current Status column provides us with the current door status, whether the door is Locked - Closed, Locked - Opened, Unlocked - Closed or Unlocked - Opened.

Manual Actions will allow us to manually Unlock the door if it is Locked and manually Lock the door if it is Unlocked. It also allows us to Momentarily Unlock the door. The Momentarily Unlock command will work only if the door is currently Locked.

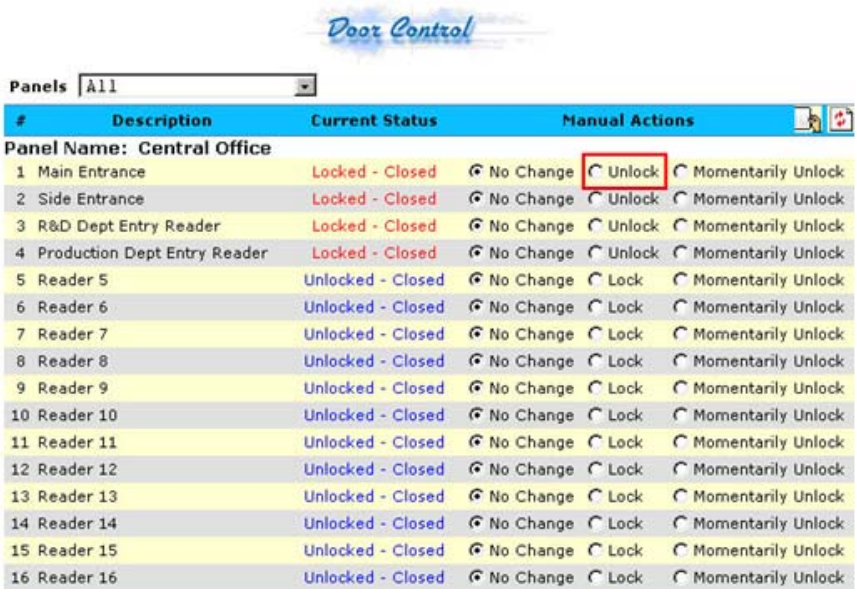
NOTICE!
Exit Readers will NOT be shown in the Door Control menu.

By default, all the Readers, except for Exit Readers, in the system will be shown on the screen. However, if you want to view a specific Controller's Readers, you could select it from

Panels All . It will list down all the on-line Controllers. Selecting a Controller from the list will cause the screen to refresh with only the readers from the selected Controller.

5.1.1 How to Unlock Reader Controlled Door

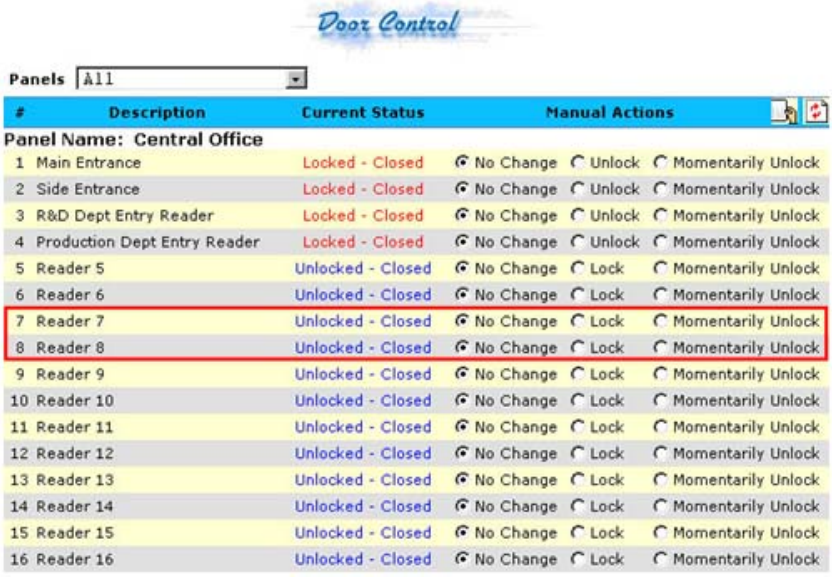
1. To unlock a specific door for an extended period of time, click on the *Unlock* radio button.


Door Control
Panels All
Description Current Status Manual Actions
Panel Name: Central Office
1 Main Entrance Locked - Closed No Change Unlock Momentarily Unlock
2 Side Entrance Locked - Closed No Change Unlock Momentarily Unlock
3 R&D Dept Entry Reader Locked - Closed No Change Unlock Momentarily Unlock
4 Production Dept Entry Reader Locked - Closed No Change Unlock Momentarily Unlock
5 Reader 5 Unlocked - Closed No Change Lock Momentarily Unlock
6 Reader 6 Unlocked - Closed No Change Lock Momentarily Unlock
7 Reader 7 Unlocked - Closed No Change Lock Momentarily Unlock
8 Reader 8 Unlocked - Closed No Change Lock Momentarily Unlock
9 Reader 9 Unlocked - Closed No Change Lock Momentarily Unlock
10 Reader 10 Unlocked - Closed No Change Lock Momentarily Unlock
11 Reader 11 Unlocked - Closed No Change Lock Momentarily Unlock
12 Reader 12 Unlocked - Closed No Change Lock Momentarily Unlock
13 Reader 13 Unlocked - Closed No Change Lock Momentarily Unlock
14 Reader 14 Unlocked - Closed No Change Lock Momentarily Unlock
15 Reader 15 Unlocked - Closed No Change Lock Momentarily Unlock
16 Reader 16 Unlocked - Closed No Change Lock Momentarily Unlock

2. Click on icon to submit/send the command.

   The selected door will now be Unlocked. Cardholders can now pass through the door without presenting a card to the Reader. The door will remain Unlocked until they are relocked. At the same time that the door is Unlocked, Access Easy Master will refresh the *Door Control screen* and update both the Current Status and the command radio buttons so they will be ready for the next command.

   The following screen shows an example of the Current Status of two doors, named Reader 7 and Reader 8, in Unlocked - Closed mode and the command radio button configured for Lock mode.


Door Control
Panels All
Description Current Status Manual Actions
Panel Name: Central Office
1 Main Entrance Locked - Closed No Change Unlock Momentarily Unlock
2 Side Entrance Locked - Closed No Change Unlock Momentarily Unlock
3 R&D Dept Entry Reader Locked - Closed No Change Unlock Momentarily Unlock
4 Production Dept Entry Reader Locked - Closed No Change Unlock Momentarily Unlock
5 Reader 5 Unlocked - Closed No Change Lock Momentarily Unlock
6 Reader 6 Unlocked - Closed No Change Lock Momentarily Unlock
7 Reader 7 Unlocked - Closed No Change Lock Momentarily Unlock
8 Reader 8 Unlocked - Closed No Change Lock Momentarily Unlock
9 Reader 9 Unlocked - Closed No Change Lock Momentarily Unlock
10 Reader 10 Unlocked - Closed No Change Lock Momentarily Unlock
11 Reader 11 Unlocked - Closed No Change Lock Momentarily Unlock
12 Reader 12 Unlocked - Closed No Change Lock Momentarily Unlock
13 Reader 13 Unlocked - Closed No Change Lock Momentarily Unlock
14 Reader 14 Unlocked - Closed No Change Lock Momentarily Unlock
15 Reader 15 Unlocked - Closed No Change Lock Momentarily Unlock
16 Reader 16 Unlocked - Closed No Change Lock Momentarily Unlock

5.1.2 How to Lock Reader Controlled Door

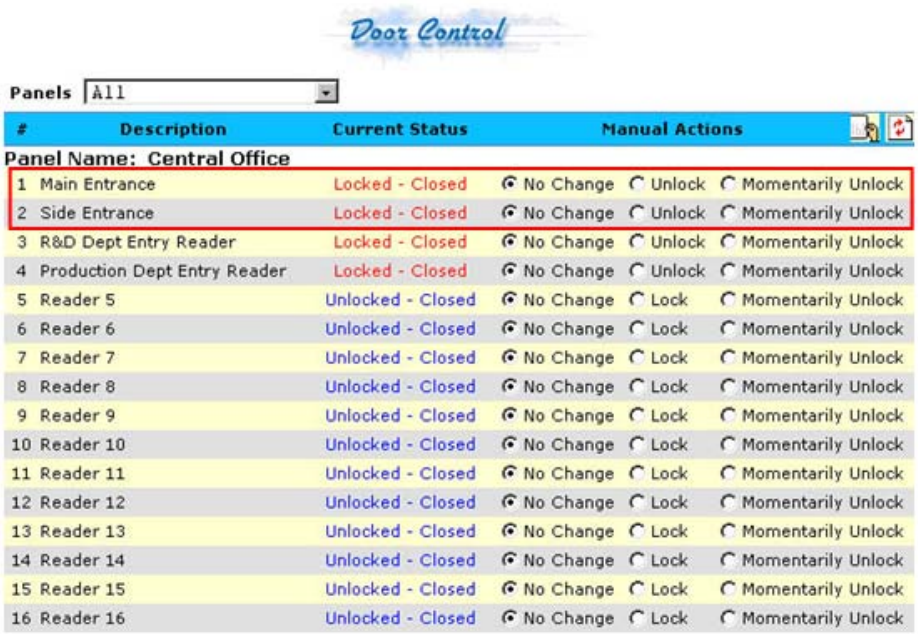
1. To lock a specific door for an extended period of time, click on the *Lock* radio button.

Door Control
Panels All
Description Current Status Manual Actions
Panel Name: Central Office
1 Main Entrance Locked - Closed No Change Unlock Momentarily Unlock
2 Side Entrance Locked - Closed No Change Unlock Momentarily Unlock
3 R&D Dept Entry Reader Locked - Closed No Change Unlock Momentarily Unlock
4 Production Dept Entry Reader Locked - Closed No Change Unlock Momentarily Unlock
5 Reader 5 Unlocked - Closed No Change Lock Momentarily Unlock
6 Reader 6 Unlocked - Closed No Change Lock Momentarily Unlock
7 Reader 7 Unlocked - Closed No Change Lock Momentarily Unlock
8 Reader 8 Unlocked - Closed No Change Lock Momentarily Unlock
9 Reader 9 Unlocked - Closed No Change Lock Momentarily Unlock
10 Reader 10 Unlocked - Closed No Change Lock Momentarily Unlock
11 Reader 11 Unlocked - Closed No Change Lock Momentarily Unlock
12 Reader 12 Unlocked - Closed No Change Lock Momentarily Unlock
13 Reader 13 Unlocked - Closed No Change Lock Momentarily Unlock
14 Reader 14 Unlocked - Closed No Change Lock Momentarily Unlock
15 Reader 15 Unlocked - Closed No Change Lock Momentarily Unlock
16 Reader 16 Unlocked - Closed No Change Lock Momentarily Unlock

2. Click on icon to submit/send the command.

   The selected door will Lock immediately. Cardholders will now be required to present their card to the Reader in order to pass though the door. At the same time that the door is Locked, Access Easy Master will refresh the Door Control screen and update both the Current Status and the command radio buttons so they will be ready for the next command.

   The following screen shows an example of the Current Status of two doors, named Main Entrance and Side Entrance, in Locked - Closed mode and the command radio button configured for Unlock mode.


Door Control
Panels All
Description Current Status Manual Actions
Panel Name: Central Office
1 Main Entrance Locked - Closed No Change Unlock Momentarily Unlock
2 Side Entrance Locked - Closed No Change Unlock Momentarily Unlock
3 R&D Dept Entry Reader Locked - Closed No Change Unlock Momentarily Unlock
4 Production Dept Entry Reader Locked - Closed No Change Unlock Momentarily Unlock
5 Reader 5 Unlocked - Closed No Change Lock Momentarily Unlock
6 Reader 6 Unlocked - Closed No Change Lock Momentarily Unlock
7 Reader 7 Unlocked - Closed No Change Lock Momentarily Unlock
8 Reader 8 Unlocked - Closed No Change Lock Momentarily Unlock
9 Reader 9 Unlocked - Closed No Change Lock Momentarily Unlock
10 Reader 10 Unlocked - Closed No Change Lock Momentarily Unlock
11 Reader 11 Unlocked - Closed No Change Lock Momentarily Unlock
12 Reader 12 Unlocked - Closed No Change Lock Momentarily Unlock
13 Reader 13 Unlocked - Closed No Change Lock Momentarily Unlock
14 Reader 14 Unlocked - Closed No Change Lock Momentarily Unlock
15 Reader 15 Unlocked - Closed No Change Lock Momentarily Unlock
16 Reader 16 Unlocked - Closed No Change Lock Momentarily Unlock

5.1.3 How to Momentarily Unlock Reader Controlled Door

1. To momentarily unlock a specific door, click on the *Momentarily Unlock* radio button.

Door Control
Panels All
Description Current Status Manual Actions
Panel Name: Central Office
1 Main Entrance Unlocked - Closed No Change Lock Momentarily Unlock
2 Side Entrance Unlocked - Closed No Change Lock Momentarily Unlock
3 R&D Dept Entry Reader Unlocked - Closed No Change Lock Momentarily Unlock
4 Production Dept Entry Reader Unlocked - Closed No Change Lock Momentarily Unlock
5 Elevator Reader Unlocked - Closed No Change Lock Momentarily Unlock
6 Reader 6 Unlocked - Closed No Change Lock Momentarily Unlock
7 Reader 7 Unlocked - Closed No Change Lock Momentarily Unlock
8 Reader 8 Unlocked - Closed No Change Lock Momentarily Unlock
9 Reader 9 Unlocked - Closed No Change Lock Momentarily Unlock
10 Reader 10 Unlocked - Closed No Change Lock Momentarily Unlock
11 Reader 11 Unlocked - Closed No Change Lock Momentarily Unlock
12 Reader 12 Unlocked - Closed No Change Lock Momentarily Unlock
13 Reader 13 Unlocked - Closed No Change Lock Momentarily Unlock
14 Reader 14 Unlocked - Closed No Change Lock Momentarily Unlock
15 Reader 15 Unlocked - Closed No Change Lock Momentarily Unlock
16 Reader 16 Unlocked - Closed No Change Lock Momentarily Unlock

2. Click on icon to submit/send the command.

The selected door will Momentarily Unlock. The door will remain Unlocked for the duration of time specified in the Reader configuration (usually 5 to 10 seconds). At the expiration of the Unlock duration, the door will automatically relock.

NOTICE!
If you Momentarily Unlock a door, you will not be able to see the true status.

5.2 Input Control

Input control allows us to check the status of all the input points and whether they are assigned to specific Alarm Zones, and to send a command to manually Arm/Disarm the input point or zone. As this is a manual control, it has priority over the controls set by the system. However the system will take over once it encounters a valid Schedule.

Devices that are usually monitored by input points are motion detectors, skylights, and temperature sensors. Besides monitoring the status of these input sensors, the Input Control screen provides an easy way for the user to arm and disarm these alarm points.

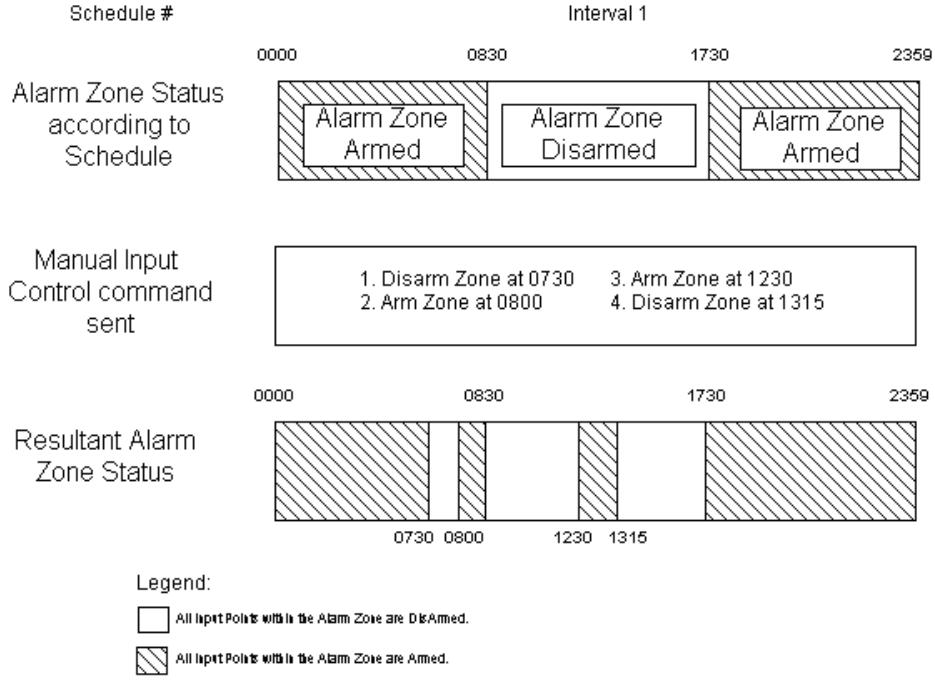
Disarming an alarm point is the same as turning it off. When an input point is disarmed, it no longer reports alarms to the Activity screen.

Arming an alarm point means that you are turning it back on. When an input point is armed, monitoring of that point is re-enabled and events from the point will once again be reported to the Activity screen.

For configuration of system control, please refer to Panels Admin, Input Setup.

Before we begin, we show an example to illustrate the operational behaviour. The setting for Interval 1 is Start - 0830hrs and End - 1730hrs.

Interval 2,3, and 4 has no setting.



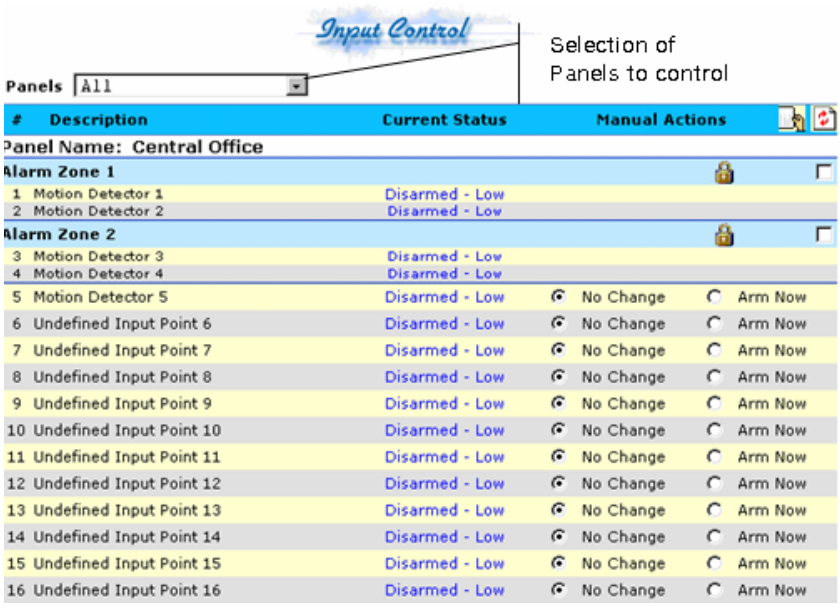
Notice that the system resumes normal operation as according to Schedule at 0830hrs and 1731hrs.

Now we are ready to control the Input Points.

1. From the Access Easy Master main menu page, click on *Input Control*.

Security Systems
Access Easy Master
BOSCH
Alarm Valid Restore All Time Attendance
View Activity
Activity
View Activity
Manual Control
Door Control
Input Control
Output Control
Card Database
Card Assignment
Access Levels
System Admin
Users Setup
Panel Setup
Holidays
Schedules
Server Setup
Report Generation
Database Backup
Reboot
Shutdown
Logout
Panels Admin
172.16.10.92
Access Groups
Card Readers
Input Setup
Output Setup
Advance I/O Setup
Input Point Configuration
Email/SMS Configuration
Reset APB
Alarm Activities
Panel No | Date | Location | Activity Description
Priority | Time | Card No | User Name
20 (2) | 23 Dec 2005 11:40:41 | Reader 2 10 | Access Denied - Passback Card Number:10
1 (1) | 23 Dec 2005 11:40:39 | Reader 3 (0)31 | Invalid Card Standard 26 bit Format
20 (2) | 23 Dec 2005 11:40:37 | Reader 1 9 | Invalid Second Card Read Card Number:9
1 (1) | 23 Dec 2005 11:40:36 | Reader 2 (0)30 | Invalid Card Standard 26 bit Format
20 (2) | 23 Dec 2005 11:40:34 | Reader 4 8 | Exit Denied - Passback Card Number:8
1 (2) | 23 Dec 2005 11:40:33 | Reader 1 29 | Invalid First Card Read Card Number:29
20 (1) | 23 Dec 2005 11:40:09 | Reader 4 (0)32 | Invalid Card Standard 26 bit Format
20 (1) | 23 Dec 2005 11:40:06 | Reader 3 (0)31 | Invalid Card Standard 26 bit Format
20 (1) | 23 Dec 2005 11:40:03 | Reader 2 (0)30 | Invalid Card Standard 26 bit Format
1 (1) | 23 Dec 2005 11:39:01 | Reader 4 (0)32 | Invalid Card Standard 26 bit Format

2. The *Input Control* screen will appear.


Input Control
Selection of Panels to control
Panels All
Description | Current Status | Manual Actions
Panel Name: Central Office
Alarm Zone 1
1 Motion Detector 1 Disarmed - Low
2 Motion Detector 2 Disarmed - Low
Alarm Zone 2
3 Motion Detector 3 Disarmed - Low
4 Motion Detector 4 Disarmed - Low
5 Motion Detector 5 Disarmed - Low No Change Arm Now
6 Undefined Input Point 6 Disarmed - Low No Change Arm Now
7 Undefined Input Point 7 Disarmed - Low No Change Arm Now
8 Undefined Input Point 8 Disarmed - Low No Change Arm Now
9 Undefined Input Point 9 Disarmed - Low No Change Arm Now
10 Undefined Input Point 10 Disarmed - Low No Change Arm Now
11 Undefined Input Point 11 Disarmed - Low No Change Arm Now
12 Undefined Input Point 12 Disarmed - Low No Change Arm Now
13 Undefined Input Point 13 Disarmed - Low No Change Arm Now
14 Undefined Input Point 14 Disarmed - Low No Change Arm Now
15 Undefined Input Point 15 Disarmed - Low No Change Arm Now
16 Undefined Input Point 16 Disarmed - Low No Change Arm Now

Description provides the grouping of the Input Point, if any. The horizontal strip in blue provides the Alarm Zone to which the Input Points belong. The Alarm Zones are separated by a blue line. Independent Input Points do not belong to any Alarm Zone. In this case, Input Point 1 & 2 belong to Alarm Zone 1. Input Point 3 & 4 belong to Alarm Zone 2. Input Point 5 is an independent input point.

The table below describes the possible grouping of the Input Point.

Alarm Zone 1	Input Points in Alarm Zone 1 are displayed together. They are to be armed / disarmed together.
Alarm Zone 2	Input Points in Alarm Zone 2 are displayed together. They are to be armed / disarmed together.
Alarm Zone 3	Input Points in Alarm Zone 3 are displayed together. They are to be armed / disarmed together.
Alarm Zone 4	Input Points in Alarm Zone 4 are displayed together. They are to be armed / disarmed together.
Independent Input Point	These are Independent Input Points which can be armed / disarmed by itself.

Current Status column provides us with the current input point status.

The table below describes the possible status of the Input Point.

Current Status	Description
Armed	The respective Input Point is Armed.
Disarmed - Low	The respective Input Point is Disarmed and its current status is closed.
Disarmed - High	The respective Input Point is Disarmed and its current status is open.
Alarm	An Alarm is detected from the Input Point.
Alarm-Restored	The alarm has been restored so that the Input Point is no longer in Alarm state.
Bypassed-Low	If the status of the Input Point is currently at Bypassed-High, after the Input Point contact is closed, it becomes Bypassed-Low.
Bypassed-High	The Input Point has been Bypassed though the Alarm Zone is Armed. This situation happens when the current status of the Input Point is open before the Input Point is armed.

Manual Actions column provides the check box for selection of the input points to issue the command.

There are 2 types of action command available:

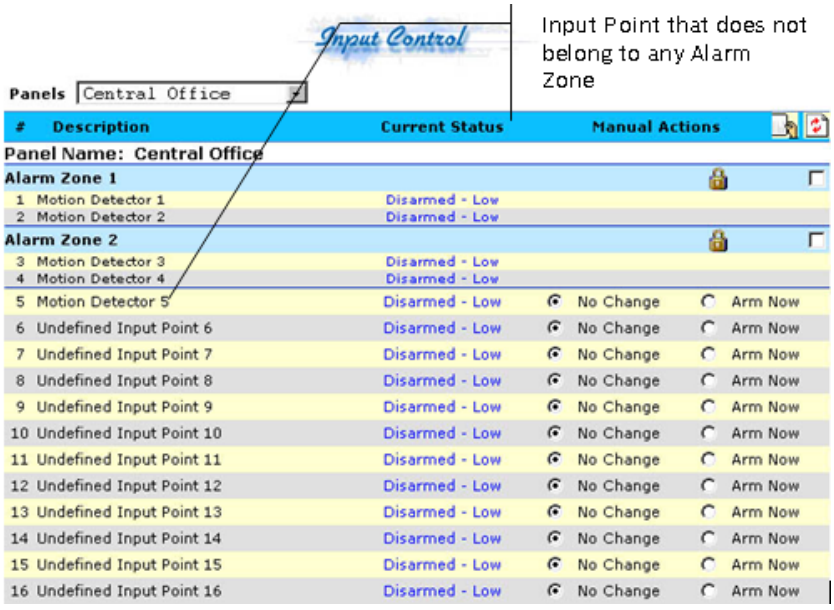
	This icon means that by selecting the check box, an Arming command will be issued when submitted. Alternatively, click on the icon to arm the Alarm Zone.
	This icon means that by selecting the check box, a Disarming command will be issued when submitted. Alternatively, click on the icon to disarm the Alarm Zone.

By default, all the inputs in the system will be shown on the screen. However, if you want to view a specific Controller's inputs, you could select it from

. It will list down all the on-line Controllers. Selecting a Controller from the list will cause the screen to refresh with only the Input Points from the selected Controller.

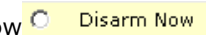
5.2.1 How to Arm/Disarm an Input Point

These are Input points that are not included in any of the 4 Alarm Zones nor is it controlled by Schedule. They are independent points that could be armed or disarmed by itself.

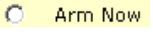

Input Control
Input Point that does not belong to any Alarm Zone
Panels Central Office
Description
Current Status
Manual Actions
Panel Name: Central Office
Alarm Zone 1
1 Motion Detector 1 Disarmed - Low
2 Motion Detector 2 Disarmed - Low
Alarm Zone 2
3 Motion Detector 3 Disarmed - Low
4 Motion Detector 4 Disarmed - Low
5 Motion Detector 5 Disarmed - Low No Change Arm Now
6 Undefined Input Point 6 Disarmed - Low No Change Arm Now
7 Undefined Input Point 7 Disarmed - Low No Change Arm Now
8 Undefined Input Point 8 Disarmed - Low No Change Arm Now
9 Undefined Input Point 9 Disarmed - Low No Change Arm Now
10 Undefined Input Point 10 Disarmed - Low No Change Arm Now
11 Undefined Input Point 11 Disarmed - Low No Change Arm Now
12 Undefined Input Point 12 Disarmed - Low No Change Arm Now
13 Undefined Input Point 13 Disarmed - Low No Change Arm Now
14 Undefined Input Point 14 Disarmed - Low No Change Arm Now
15 Undefined Input Point 15 Disarmed - Low No Change Arm Now
16 Undefined Input Point 16 Disarmed - Low No Change Arm Now

1. Select the desired radio button (see NOTICE below).
2. Click on the button to send the command.The web page will refresh to reflect the new status.

NOTICE!

If the current status of the Input Point is Armed, the Manual Actions will show 

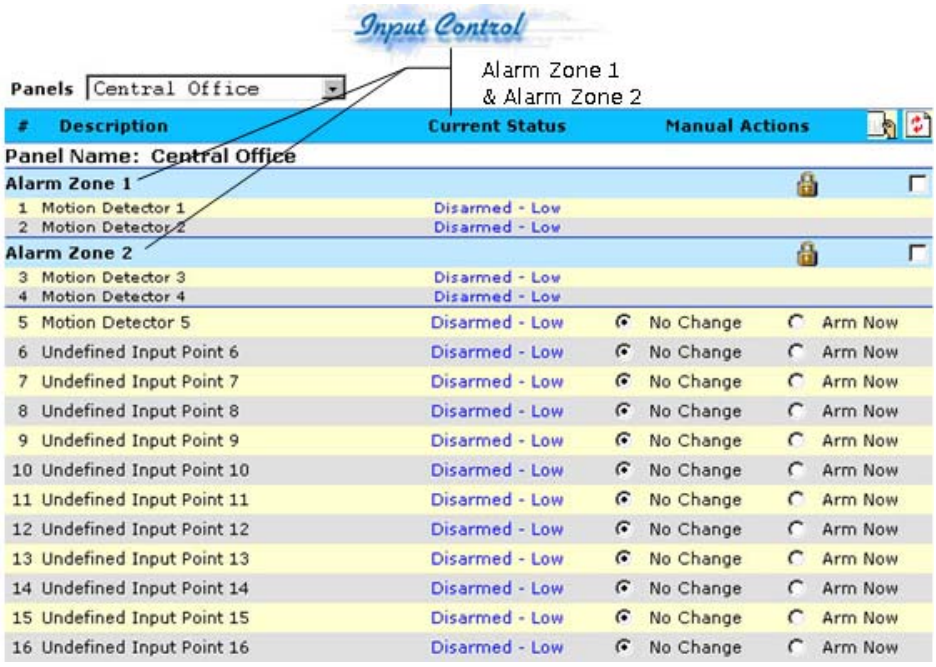
, which means you could send a disarm command to this input when the button is click.

Likewise, if the Input Point is currently Disarmed, the Manual Actions will show 

.

5.2.2 How to Arm an Alarm Zone

Input Points can be grouped together if they are to be Armed/Disarmed together. This forms a group which is known as Alarm Zone. In each of the Access Easy Controller, it allows up to 4 Alarm Zones. These Alarm Zones can be Armed/Disarmed by means of Arm/Disarm Readers or from the *Input Control* screen. Access Easy Master consolidates all the Alarm Zones from each individual Access Easy Controller that it is managing in a single screen. User could Arm/Disarm any Alarm Zone directly from this screen. The following screen shows an example of the *Input Control* screen with Alarm Zone 1 and Alarm Zone 2 from a Access Easy Controller called Central Office.


Input Control
Panels Central Office
Alarm Zone 1
& Alarm Zone 2
# Description
Current Status
Manual Actions
Panel Name: Central Office
Alarm Zone 1
1 Motion Detector 1 Disarmed - Low
2 Motion Detector 2 Disarmed - Low
Alarm Zone 2
3 Motion Detector 3 Disarmed - Low
4 Motion Detector 4 Disarmed - Low
5 Motion Detector 5 Disarmed - Low No Change Arm Now
6 Undefined Input Point 6 Disarmed - Low No Change Arm Now
7 Undefined Input Point 7 Disarmed - Low No Change Arm Now
8 Undefined Input Point 8 Disarmed - Low No Change Arm Now
9 Undefined Input Point 9 Disarmed - Low No Change Arm Now
10 Undefined Input Point 10 Disarmed - Low No Change Arm Now
11 Undefined Input Point 11 Disarmed - Low No Change Arm Now
12 Undefined Input Point 12 Disarmed - Low No Change Arm Now
13 Undefined Input Point 13 Disarmed - Low No Change Arm Now
14 Undefined Input Point 14 Disarmed - Low No Change Arm Now
15 Undefined Input Point 15 Disarmed - Low No Change Arm Now
16 Undefined Input Point 16 Disarmed - Low No Change Arm Now

How to Arm an Alarm Zone :

Click on to Arm the Alarm Zone immediately. The icon indicates that the Alarm Zone is currently disarmed.

How to Disarm an Alarm Zone :

Click on to Disarm the Alarm Zone immediately. The icon indicates that the Alarm Zone is currently armed.

How to Arm/Disarm a Group of Alarm Zones :
If you want to Arm/Disarm multiple Alarm Zones, select the Alarm Zones that you want to Arm/

Disarm by ticking on the check boxes and clicking on the submit icon.

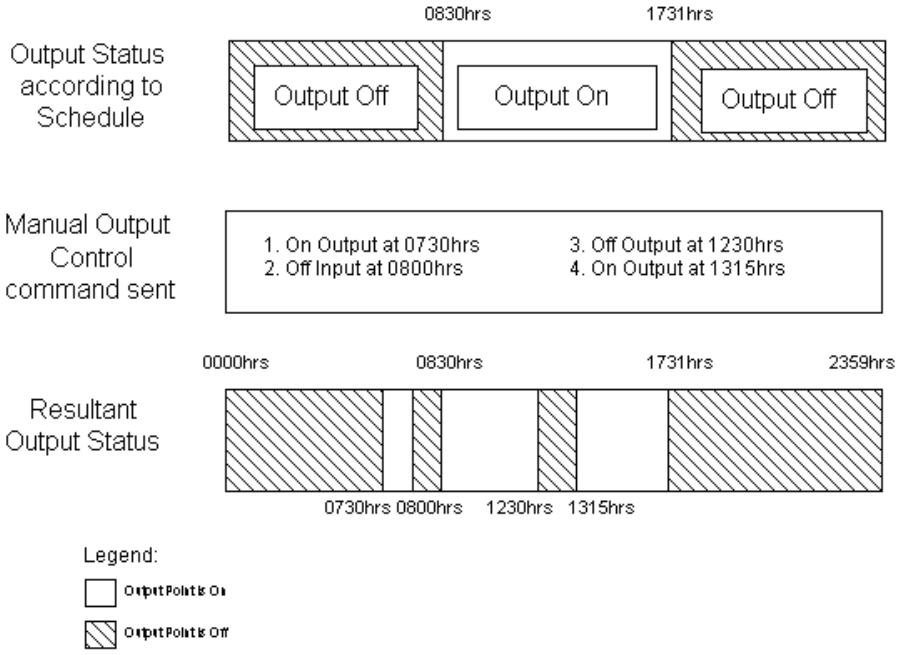
5.3 Output Control

The *Output Control* is one of the menu items of the *Manual Control* Group. It allows user to check the status of all the Output Points and send a command to turn On/Off the points manually. However, if the Output Point is linked to an Input Point as a Status Output, the status will not be indicated here.
Devices that can be controlled by the Output Points are alarm bells, lighting circuits, electric garage door openers, etc. Essentially, any device that can be turned On and Off can be controlled by the *Output Control*.

As this is a control operated by a user manually, it has priority over the control set by the system. However, the system will take over and resume normal operation once it encounters a valid Schedule interval.

For configuration of system control, please refer to *Panels Admin, Output Setup*.

Before we begin, we show an example to illustrate the operational condition.
The setting for Interval 1 is Start - 0830hrs and End - 1730hrs.
Interval 2,3, and 4 has no setting.



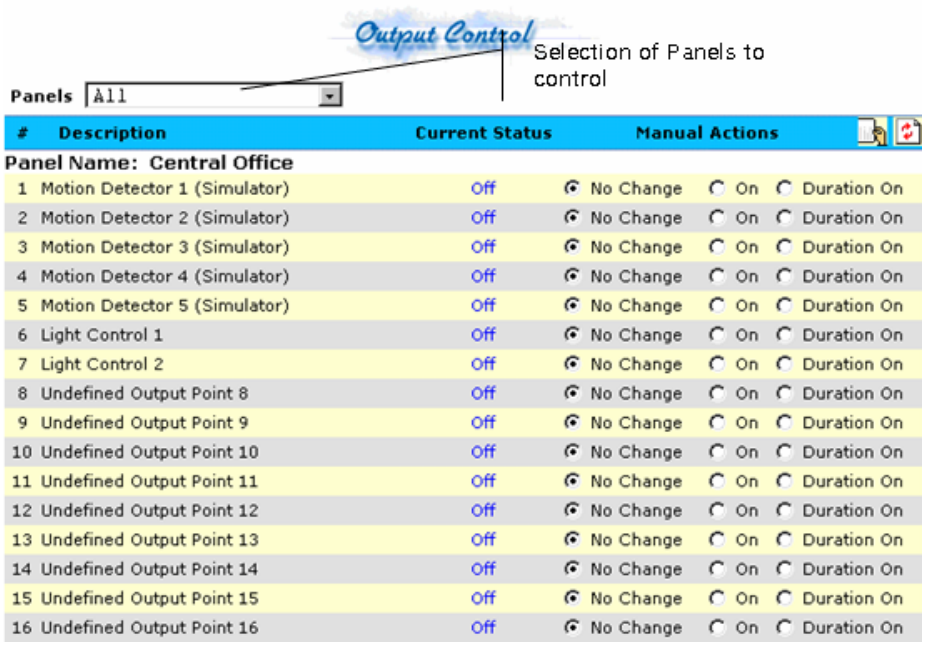
Notice that the system resumes normal operation as according to Schedule at 0830hrs and 1731hrs.

Now let us continue with the Output Control.

1. From the Access Easy Master main menu page, click on *Output Control*.

Security Systems
Access Easy Master
BOSCH
Activity
View Activity
Manual Control
Door Control
Input Control
Output Control
Card Database
Card Assignment
Access Levels
System Admin
Users Setup
Panel Setup
Holidays
Schedules
Server Setup
Report Generation
Database Backup
Reboot
Shutdown
Logout
Panels Admin
172.16.10.92
Access Groups
Card Readers
Input Setup
Output Setup
Advance I/O Setup
Input Point Configuration
Email/SMS Configuration
Reset APB
Alarm Valid Restore All Time Attendance
View Activity
Alarm Activities
Panel No | Date | Location | Activity Description
Priority | Time | Card No | User Name
20 (2) | 23 Dec 2005 11:40:41 | Reader 2 10 | Access Denied - Passback Card Number:10
1 (1) | 23 Dec 2005 11:40:39 | Reader 3 (0)31 | Invalid Card Standard 26 bit Format
20 (2) | 23 Dec 2005 11:40:37 | Reader 1 9 | Invalid Second Card Read Card Number:9
1 (1) | 23 Dec 2005 11:40:36 | Reader 2 (0)30 | Invalid Card Standard 26 bit Format
20 (2) | 23 Dec 2005 11:40:34 | Reader 4 8 | Exit Denied - Passback Card Number:8
1 (2) | 23 Dec 2005 11:40:33 | Reader 1 29 | Invalid First Card Read Card Number:29
20 (1) | 23 Dec 2005 11:40:09 | Reader 4 (0)32 | Invalid Card Standard 26 bit Format
20 (1) | 23 Dec 2005 11:40:06 | Reader 3 (0)31 | Invalid Card Standard 26 bit Format
20 (1) | 23 Dec 2005 11:40:03 | Reader 2 (0)30 | Invalid Card Standard 26 bit Format
1 (1) | 23 Dec 2005 11:39:01 | Reader 4 (0)32 | Invalid Card Standard 26 bit Format

2. The *Output Control* screen will appear.


Output Control
Selection of Panels to control
Panels All
Description Current Status Manual Actions
Panel Name: Central Office
1 Motion Detector 1 (Simulator) Off No Change On Duration On
2 Motion Detector 2 (Simulator) Off No Change On Duration On
3 Motion Detector 3 (Simulator) Off No Change On Duration On
4 Motion Detector 4 (Simulator) Off No Change On Duration On
5 Motion Detector 5 (Simulator) Off No Change On Duration On
6 Light Control 1 Off No Change On Duration On
7 Light Control 2 Off No Change On Duration On
8 Undefined Output Point 8 Off No Change On Duration On
9 Undefined Output Point 9 Off No Change On Duration On
10 Undefined Output Point 10 Off No Change On Duration On
11 Undefined Output Point 11 Off No Change On Duration On
12 Undefined Output Point 12 Off No Change On Duration On
13 Undefined Output Point 13 Off No Change On Duration On
14 Undefined Output Point 14 Off No Change On Duration On
15 Undefined Output Point 15 Off No Change On Duration On
16 Undefined Output Point 16 Off No Change On Duration On

Description provides the Controller Name and the Output Points allocated to it.

Current Status provides us with the current status of the Output Points. On status indicates that the Output Point is currently activated and Off status indicates that the Output Point is currently not activated.

Manual Actions provide us with radio buttons for performing manual actions. The next radio button is for toggling the status between On/Off.
There are 4 types of action command available :

On	Selecting the radio button next to it will send a command to turn On the Output Point when submitted.
Off	Selecting the radio button next to it will send a command to turn Off the Output Point when submitted.
Duration On	Selecting the radio button next to it will send a command to turn On the Output Point for a pre-defined Duration when submitted.
Duration Off	Selecting the radio button next to it will send a command to turn Off the Output Point for a pre-defined Duration when submitted.

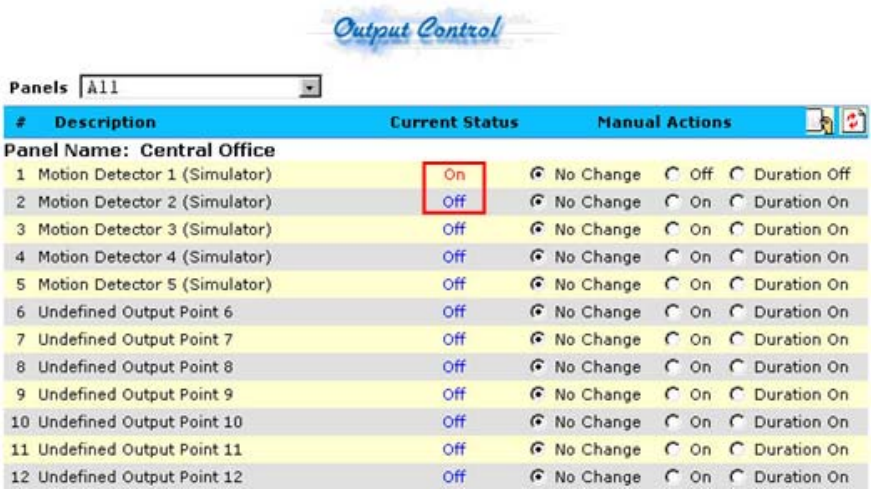
The pre-defined duration for the Duration On and Duration Off is determined in the Duration field in *Panels Admin, Output Setup*.

By default, all the outputs in the system will be shown on the screen. However, if you want to view a specific Controller's outputs, you could select it from

. It will list down all the on-line Controllers. Selecting a Controller from the list will cause the screen to refresh with only the Output Points from the selected Controller.

5.3.1 How to Turn On/Off Output Points

1. To activate the selected Output Point, click the On or Off icon.


Output Control
Panels All
Description Current Status Manual Actions
Panel Name: Central Office
1 Motion Detector 1 (Simulator) On No Change Off Duration Off
2 Motion Detector 2 (Simulator) Off No Change On Duration On
3 Motion Detector 3 (Simulator) Off No Change On Duration On
4 Motion Detector 4 (Simulator) Off No Change On Duration On
5 Motion Detector 5 (Simulator) Off No Change On Duration On
6 Undefined Output Point 6 Off No Change On Duration On
7 Undefined Output Point 7 Off No Change On Duration On
8 Undefined Output Point 8 Off No Change On Duration On
9 Undefined Output Point 9 Off No Change On Duration On
10 Undefined Output Point 10 Off No Change On Duration On
11 Undefined Output Point 11 Off No Change On Duration On
12 Undefined Output Point 12 Off No Change On Duration On

2. Click on icon to submit the command.

Clicking on the icon will refresh the web page and reflect its new status.

NOTICE!

If the current status of the Output Point is Off, the Manual Action will show On, which means you could send a On command to this output when the button is clicked. Likewise, if the Output Point is currently On, the Manual Action will show Off.

6 Card Assignment

This Chapter describes the features of the Card Assignment function and the set up procedure.

Card parameters are parameters that control the use of cards. It contains information such as which card reader a cardholder can access at specified *Schedule*. There will be some extra fields for user to configure additional card information like Department and User Fields. *Card Assignment* consists of the following parameters: -

- Card Details
  a. Card Number
  b. Facility Code
  c. Card Format
  d. User Name
  e. Department
  f. User Field 1
  g. User Field 2
  h. Access Level

- Card Functionality
  a. Whether cardholder is able to Arm/Disarm
  b. Whether cardholder must abide by Holiday Schedules
  c. Whether to allow exit reader usage only in accordance with time schedules
  d. Whether Card + Pin is required on keypad readers
  e. Whether cardholder is One Time Access only, with the Access Status as Valid or Expired
  f. Setting of User Pin (1 ~ 7 digits)
  g. Setting of Extended duration for door access
  h. Card Validation Dates
  i. Dual Card Assignment

Assignment of Cards is done in the *Card Assignment* page. Click on *Card Assignment* from the Main Menu to see the list of currently configured cards.

In the Access Easy Master, cards that are added will be synchronized to all the on-line Controllers at the moment the cards are added. If a new Controller is connected to the Access Easy Master only after the cards are added, user will have to manually synchronize the card database to the Controller by clicking on the button for that Controller, in the *Panel Setup* page. Please refer to *Chapter 9 Panel Setup* for details.

Cards that are added allow its cardholder to access doors from different Access Easy Controllers that are managed by the Access Easy Master, provided the Access Levels, Access Groups and Schedules are properly configured.

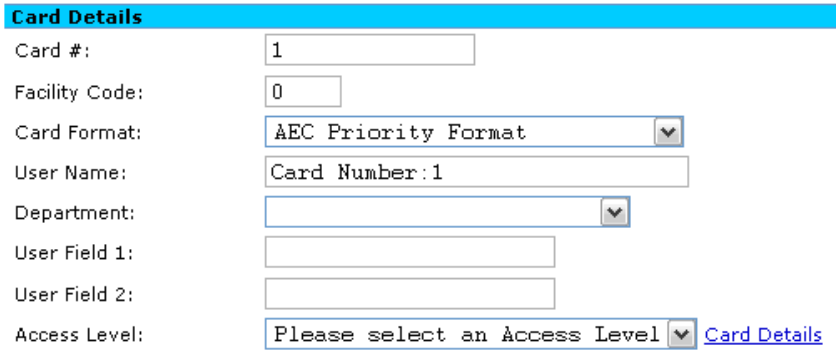
6.1 The Card Parameters

Each Card has its own field that identifies its operation and usage. We will need to pre-configure these fields properly before it can be used by the cardholder.

The *Card Assignment* screen is divided into 2 sections, Card Details and Card Functionality. The Card Details contain the settings to identify the card and the kind of access it has, while the Card Functionality contains the settings of the operation and usage.

6.1.1 Card Details

Card Details consists of the Card Number, Facility Code, Card Format, User Name, Cardholder's Department, Access rights and 2 configurable user fields, User Field 1 and 2, as shown below.



Card Number
This field contains the Card Number, it is the number that is printed on the card itself. Depending on the Card format, this number could range from 1 to any number.

For example:
Standard 26 bit wiegand format cards could only have a range of numbers from 0 to 65535.

Facility Code
This code prevents unauthorised card with the same Card Number to access your system. Some customers practise using a unique facility code that is controlled by the manufacturer. This gives additional security over the entire system. Ask your card supplier what is the facility code for your card. Without this code, the system will not be able to recognise your card.

Similar to the Card Number, the range of numbers for this code is dependent on the Card format used.

For example:
Standard 26 bit wiegand format could have a range from 0 to 255.

Card Format
Access Easy Master is able to support up to a maximum of 15 user definable Card formats. By default, AEC Priority Format and Standard 26 bit Format is pre-configured into the system. Refer to *Chapter 12 Server Setup, Card Format* for details on the configuration of card formats.

User Name
This field contains the name of the Cardholder.

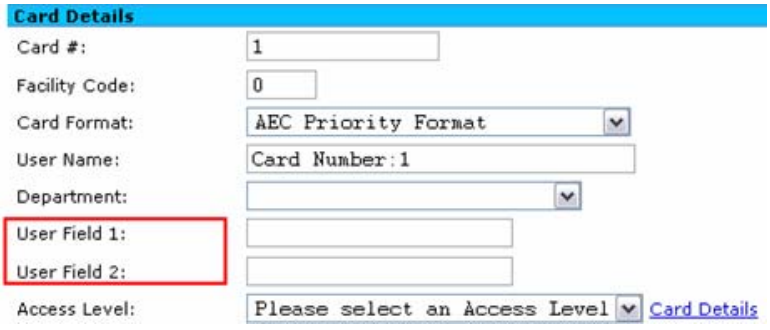
Department

This field contains the department in which the Cardholder belongs to. Access Easy Master is able to support up to a maximum of 255 user definable departments. Refer to Chapter 12 Server Setup, Company Profile, How to Edit the Department List for details on the configuration of departments.

User Field 1 & 2

These two fields are user configurable fields, it can be configured to hold non operation data such as mobile number, home contact number, office extension number, destination, staff ID, etc. Refer to *Chapter 12 Server Setup, Default Settings*, *How to Edit the User Definable Fields* for details on the configuration of User Field 1 and 2.

For example:
User Field 1 is configured as Mobile number.
User Field 2 is configured as Home contact number.
On the *Card Assignment* page, user will see User Field 1 replaced by Mobile number, and User Field 2 replaced by Home contact number, as shown below.



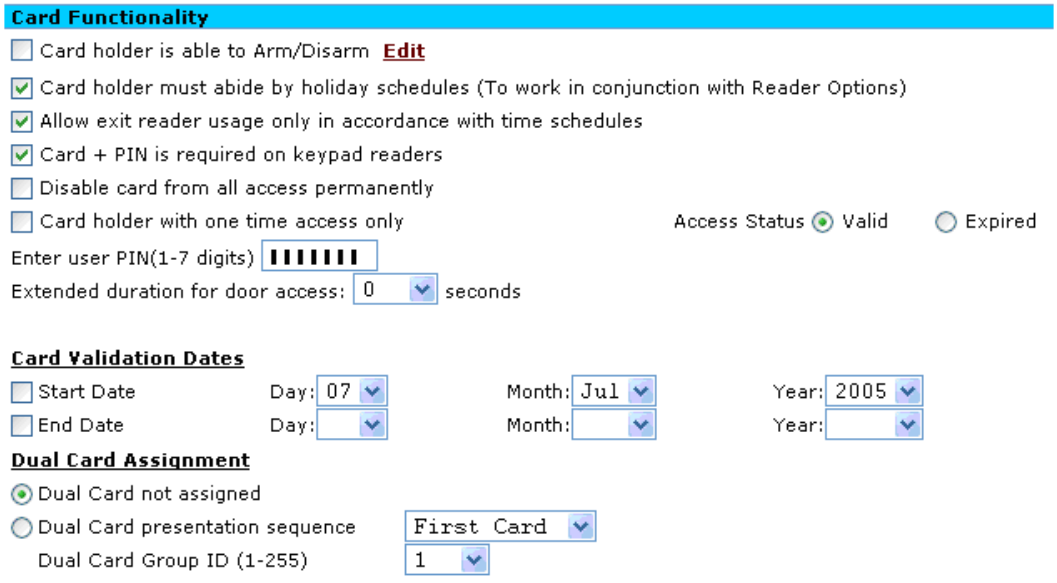
Access Level

In order to control the accessibility of doors for each Cardholder, an Access Level is assigned to each card. Each Access Level consists of one or more Access Group from different Access Easy Controller. An Access Group is a list of readers within certain authorised time periods (pre-defined Schedule) that the cardholders can access.

Access Easy Master has up to 1024 user definable Access Levels. Please refer to *Chapter 7 Access Levels* for details on the configuration of Access Levels.

Card Functionality

Card Functionality consists of the Arm/Disarm access rights, access behaviour, validation dates and dual card assignment status. Each card can be configured to behave differently. However, some settings would only be activated with the co-ordination of the *Card Readers* parameters such as Card + PIN mode and Cardholder must abide by holiday schedules. The screen below shows the card functionality for a user.


Card Functionality
Card holder is able to Arm/Disarm Edit
Card holder must abide by holiday schedules (To work in conjunction with Reader Options)
Allow exit reader usage only in accordance with time schedules
Card + PIN is required on keypad readers
Disable card from all access permanently
Card holder with one time access only
Access Status Valid Expired
Enter user PIN(1-7 digits)
Extended duration for door access: 0 seconds
Card Validation Dates
Start Date Day: 07 Month: Jul Year: 2005
End Date Day: Month: Year:
Dual Card Assignment
Dual Card not assigned
Dual Card presentation sequence First Card
Dual Card Group ID (1-255) 1

Cardholder is able to Arm/Disarm

If this feature is checked, it implies that the cardholder is given the authority to arm/disarm a specific Alarm Zone or all Alarm Zones using his card on the Zone's Arm/Disarm reader. To select an Alarm Zone, click on the *Edit* hyperlink beside Card holder is able to Arm/Disarm **Edit** . The arm/disarm details will appear as shown below.

Arm/Disarm Details
Central Office None Alarm Zone 1 Alarm Zone 2 Alarm Zone 3 Alarm Zone 4 All Zones
North Zone Branch None Alarm Zone 1 Alarm Zone 2 Alarm Zone 3 Alarm Zone 4 All Zones

Select the Alarm Zone the cardholder can Arm/Disarm for each Access Easy Controller (Central Office and North Zone Branch in this case) by selecting the appropriate radio buttons and click . If the cardholder can Arm/Disarm all the alarm zones, select the All Zones radio button. If not required, select the None radio button. To close the window, click .

NOTICE!
If cardholder has access rights to the arm/disarm reader, he has to press <0> on the reader keypad before he presents his arm/disarm card, else reader will only grant him access. In addition, user will also be granted access at the moment he disarms the Alarm Zone at the reader if he has access rights to the arm/disarm reader.

The reader must be configured as an Entry and Arm/Disarm reader for the specified zone before the cardholder can arm/disarm the Alarm Zone at the reader.

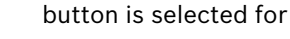
Cardholder must abide by holiday schedules (to work in conjunction with Reader Options)
This mode must be checked if the cardholders' access rights are different during holidays, either Regular Holidays or Special Holidays. This mode works in conjunction with the Reader Options, On Holidays, follow holiday schedules (to work in conjunction with card functionality). If the Reader Option is not checked, cardholders' access rights to the readers will follow the schedule for normal days of the week. Reader Options can be configured under *Panels Admin, Card Readers* of the selected Access Easy Controller menu.

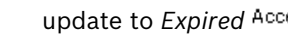
Allow exit reader usage only in accordance with time schedules
This mode is useful in case an exit reader is present. If you select this mode, the Reader will allow the cardholders to exit within their schedule intervals. If this mode is not selected, the cardholders can exit at all times, regardless of Holidays or schedules.

Card + PIN is required on Keypad readers
When this mode is selected, user will have to assign a user PIN to the card at the location Enter user PIN (1-7 digits). If this mode is selected, cardholders will have to present their card first before entering their PIN code to gain access at the reader before the Keypad Timeout, configured in the page *Panels Admin, Card Readers, Reader Options*.

Disable card from all access permanently
When this mode is selected, user card will be denied access from the system. This feature is useful to prevent illegal access to the system should the user lost/misplaced the card

Cardholder with one time access only
This will enable the administrator to assign card holder with only one time access to the system. This means that after the card holder has gained access, his access will become invalid immediately. To gain access, he needs to request the administrator to reactivate the one time access right again.

To enable this mode, check *Cardholder with one time access only*. Ensure that the Valid radio button is selected for Access Status 

. After the card has been used for one time access, the Access Status will expire immediately and the Access Status will update to *Expired* 

.

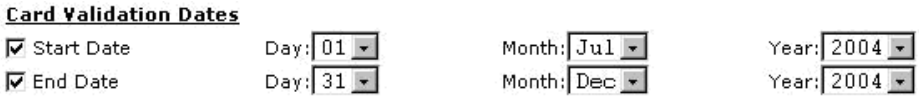
Enter user PIN (1-7 digits)
User PIN is to be used together with the Card+PIN mode. This field will contain up to maximum 7 digit.

Extended duration for door access
This function is to facilitate special card holders to have extended duration for Door Strike and Keypad Timeout. This feature will allow the cardholder to keep the door open for a longer time after a successful access grant before a Door Held Open alarm is activated. The Keypad Timeout duration is also extended by the selected time on top of the normal Keypad Timeout duration. An example of such an application is for the handicapped person who needs a longer time to access the door.

To select the extended time duration, select the time in seconds on the list box

beside the *Extended duration for door access*. The range is from 0 to 255 seconds.

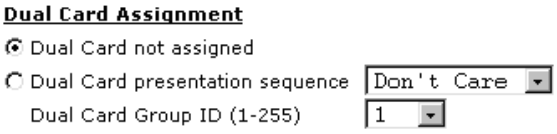
Card Validation Dates
This feature defines the start and end date parameters.



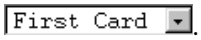
The Start Date is the date from which the card is valid and End Date is the date from which the card is no longer valid. The card will not be able to access any door before the Start Date and after the End Date

NOTICE!
User must check the respective box for Start Date or End Date in order for it to be effective.

Dual Card Assignment
This mode is useful if 2 cards are required to be presented in sequence to the Reader to unlock the door. The First Card has to be presented first before the Second Card is presented, else the door will not unlock. A Don't Care Card can act as the first or second card. In this setup here, the user will need to define whether a card is a First Card, Second Card or Don't Care Card, and which group it belongs to. Cards from different groups cannot unlock the door.



Select the radio button *Dual Card presentation sequence* to enable this mode. User will need to define whether a card is a First Card, Second Card or Don't Care Card from the list box



. User will also have to select the *Dual Card Group ID* from the list box

. 2 cards from the same Dual Card Group ID must be presented to the Reader to unlock the door. All the possible card combinations that can be presented to the Reader is shown in the table on the following page.

Possible card combination	
First card	Second Card
Don't Care	Don't Care
First Card	Don't Care
Don't Care	Second Card
First Card	Second Card

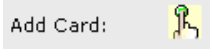
This mode works in conjunction with *Card Access Admin, Card Readers, Dual Card Configuration* of the Access Easy Controller. Please ensure that the setting in the Access Easy Controller is configured properly.

NOTICE!
For the first combination in the table above, the *Don't Care cards* must be 2 different cards from the same *Dual Card Group ID*.

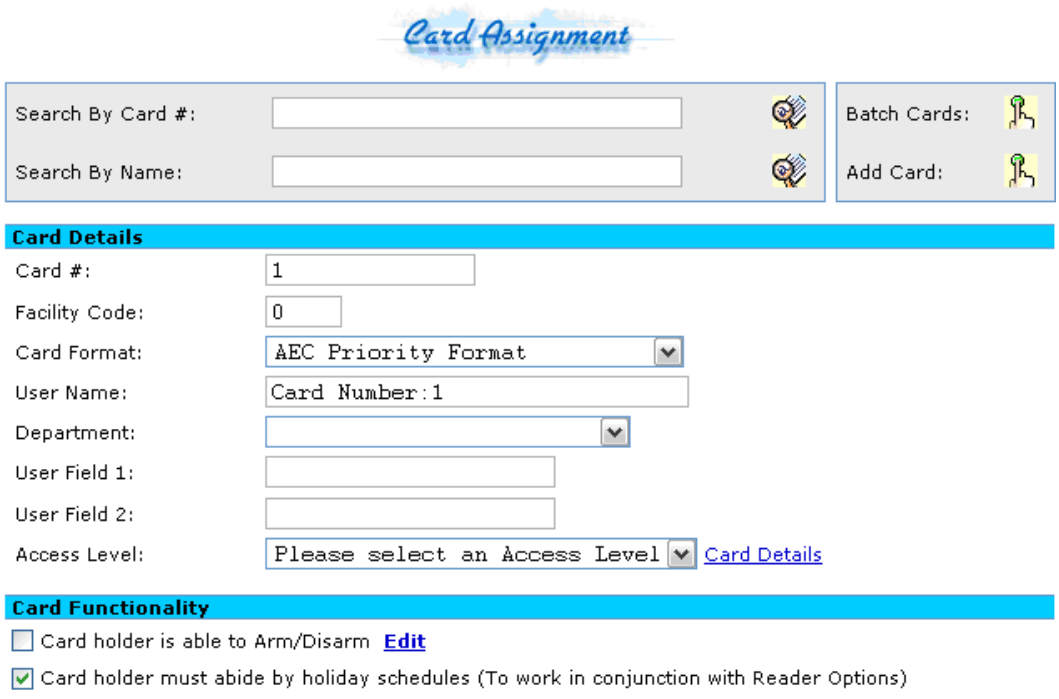
6.2 Adding and Deleting Cards

This section will describe *How to Add a New Card, How to Add a Batch of Cards* and *How to Delete a Batch of Cards*. Under the section *How to Add a Batch of Cards*, user will also learn *How to Add a Batch of Cards with Reference to an Existing Card, How to Use Automatically replace the existing card(s) with default/reference card information* and what happens during an *Unsuccessful Card Add Operation*.

6.2.1 How to Add a New Card

In the *Card Assignment* screen, click on 

to add a new card. The *Card Assignment* screen will appear as shown below.



Enter the fields in the appropriate boxes and click to save the settings. The functionality of each field is described in the section *The Card Parameters* above.

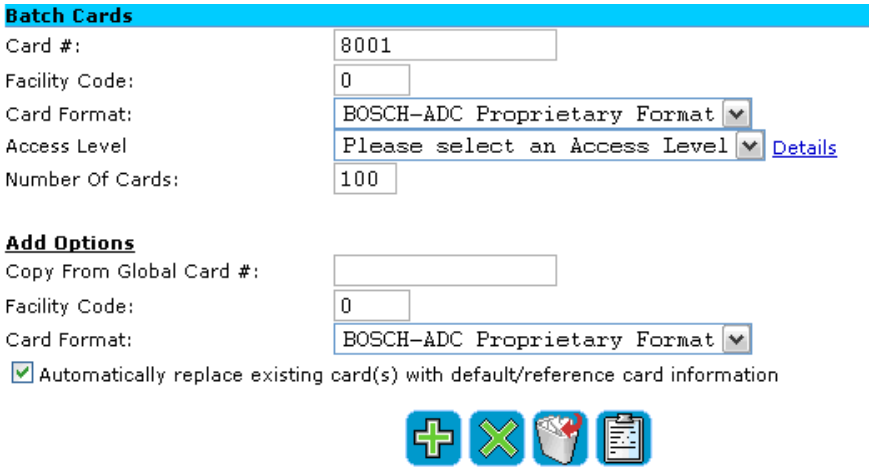
NOTICE!
During a Add Card Operation, when adding card numbers beginning with a digit 0, for example 09, the 0 will be truncated and the card number becomes 9.

6.2.2 How to Add a Batch of Cards

In the *Card Assignment* you are allowed to add a batch of cards all in a single process. This is extremely useful when a large group of cardholders is to be entered into the system at the shortest period of time. The following steps guide you how to perform this operation.

Let us take an example, presuming you need to add a batch of cards with the number ranging from 8001 to 8100.

1. Click on the icon for Batch Cards on the *Card Assignment* screen. The screen on the following page shows the default settings when Batch Cards is selected.



2. Enter the starting card ID in the *Card #* field (the number specified here will be the starting number of the batch card operation and will be included). In this example, enter 8001.
3. The number that appears in the Facility Code is configured in *Server Setup, Default Settings*. If the code is different from the default, then change it. Enter 0 if the Card Format doesn't support Facility Code.
4. Select the appropriate Card Format from the list. The configuration of the Card Format is carried out under the *Server Setup, Card Format*. Only Card Formats that have been configured will appear in the drop-down list box. By default, BOSCH-ADC Proprietary and Standard 26 bit Format is pre-configured into the system.
5. Select the Access Level for the card in the *Access Level* field. Only Access Levels that have at least one Controller selected will appear in the Access Level drop down box.
6. Enter the number of card(s) to add in the *Number of Cards* field. For this example, enter 100.
7. Click on the icon. When the add operation is in progress, a message as shown below appears.

8. If the operation is successful, a message *Batch operation completed* as shown below appears.

9. Click on the icon to go back to the *Batch Cards* menu or wait for a few seconds for the screen to return to *Batch Cards* menu automatically.
10. Click on the icon to return to the first page of *Card Assignment*.

How to Add a Batch of Cards with Reference to an Existing Card

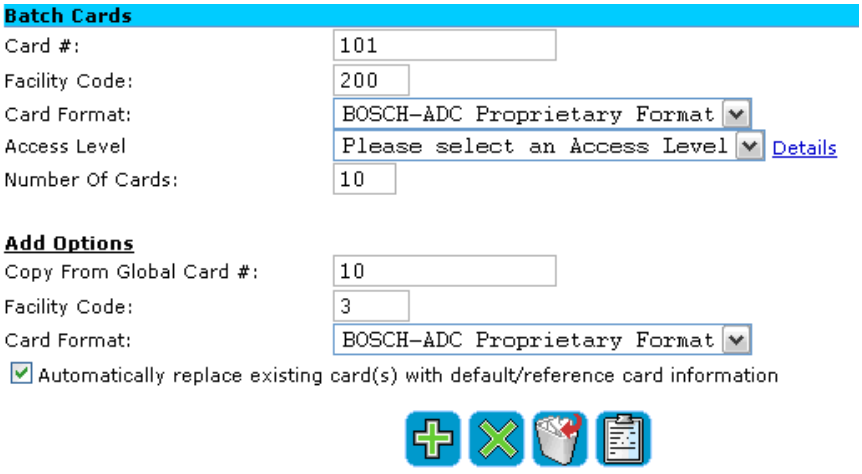
This function allows addition of a range of card numbers with data entries copied from a reference card number. All card number(s) added will be copied with the data / parameters of the reference card.

NOTICE!

Parameters such as Facility Code, Card Format, User Name and Access Level will not be copied, as all these parameters relate to the individual cardholder.

Consider an example. To assign cards with numbers from 101 to 110 to certain staffs. This range of cards have the Facility Code of 200 and of Standard 26 bit Card Format. Using card number 10 of Facility Code 3 and BOSCH-ADC Proprietary Card Format to be our reference card for the new card setting, we proceed as follows.

1. Click on the icon for *Batch Cards* and enter the relevant fields as shown.



2. Click on the icon to proceed. If there is no error during the card numbers addition, the *Batch operation completed message* would be shown.

How to Use Automatically replace the existing card(s) with default/reference card information function

This function will overwrite all data within a card number when the software encounters existing card number (with same Card Format, Facility Code and Card Number) during *Batch Cards* function. It allows recycling of card number allocation when employee resigns.

The function will be activated when a tick appears in the check box *Automatically replace existing card(s) with default/reference card information*.

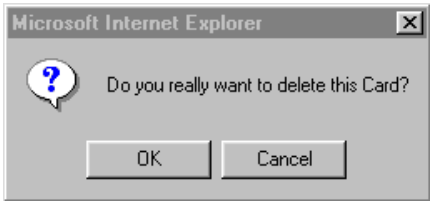
Unsuccessful Card Add Operation

There are a few occasion when the Card Add Operation is not successful. When this occurs, the following messages will be displayed on the screen.

Card No already exist	An existing card with the same *Card Number, Facility Code* and *Card Format* is found in the system and *Automatically replace existing card(s) with default/reference card information* option is not selected. The system will not overwrite the existing card and the new card will not be added.
Reference card number not found	Reference card is not found in the database. It could be due to incorrect information in *Card Format, Facility Code* or *Card Number*.

6.2.3 How to Delete a Batch of Cards

1. You can delete a range of card numbers in a way similar to adding cards. Click on the icon instead to delete card numbers.
2. A window as shown below appears. Select [OK] to delete cards.



3. After the cards are successfully deleted, a *Batch operation completed message* appears.

NOTICE!

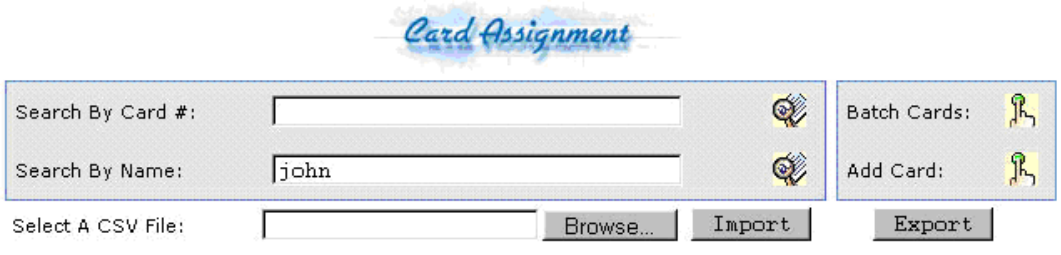
Deleting a range of cards is irreversible, so you have to be careful while deleting.

6.3 How to Import and Export Card Database

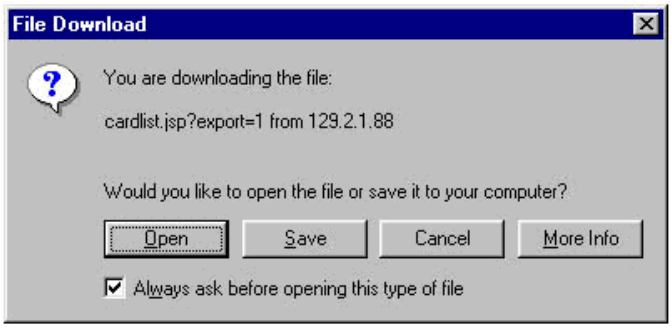
Card Database can be exported in CSV format to be stored in the user's PC. Users can then make changes to the file and import the amended file into the system.

6.3.1 How to Export the Card Database

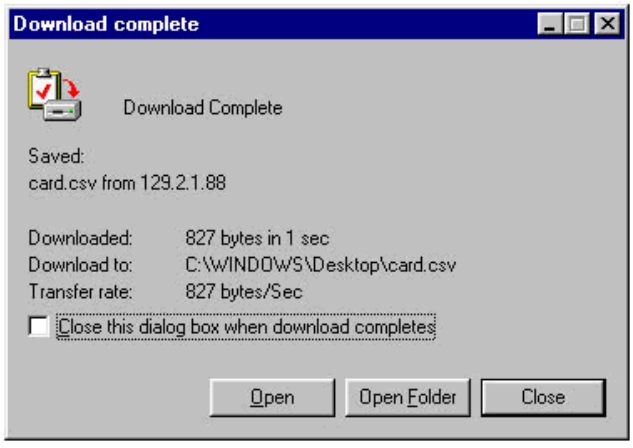
1. On the first page of Card Assignment, click on the Export button located below the Add Card function, as shown below.



2. The *File Download* box would appear, as shown below.

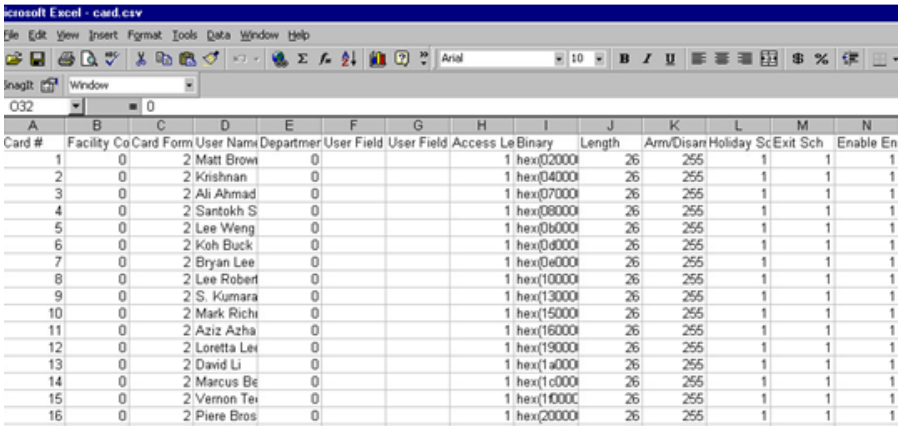

File Download
You are downloading the file:
cardlist.jsp?export=1 from 129.2.1.88
Would you like to open the file or save it to your computer?
Open
Save
Cancel
More Info
Always ask before opening this type of file

3. Click on the [Save] button to save the card database to your computer or click on the [Open] button to open the file.
4. If the [Save] button is clicked, after the download is successful, the *Download Complete* box appears, as shown below.



5. Click on the [Close] button to close the box or click on the [Open] button to open the downloaded file.

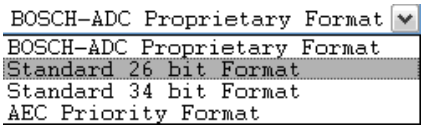
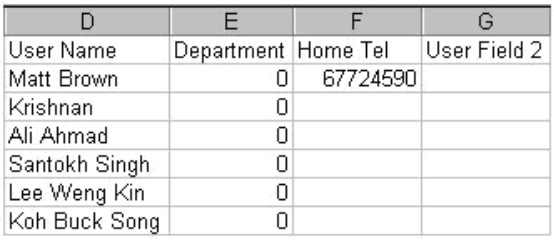
A sample of the CSV file saved is as shown below.



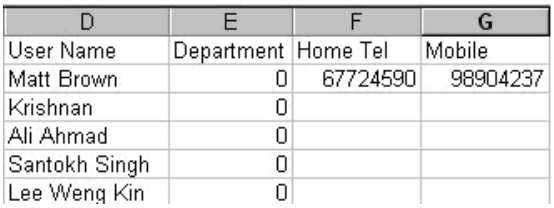
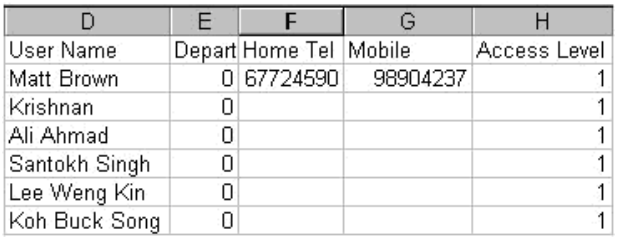
Card #	Facility Co	Card Form	User Nam	Departmer	User Field	User Field	Access Le	Binary	Length	Arm/Disar	Holiday Sc	Exit Sch	Enable En
1	0	2	Matt Brow	0			1	hex(02000	26	255	1	1	1
2	0	2	Krishnan	0			1	hex(04000	26	255	1	1	1
3	0	2	Ali Ahmad	0			1	hex(07000	26	255	1	1	1
4	0	2	Santokh S	0			1	hex(08000	26	255	1	1	1
5	0	2	Lee Weng	0			1	hex(0b000	26	255	1	1	1
6	0	2	Koh Buck	0			1	hex(0d000	26	255	1	1	1
7	0	2	Bryan Lee	0			1	hex(0e000	26	255	1	1	1
8	0	2	Lee Robert	0			1	hex(10000	26	255	1	1	1
9	0	2	S. Kumara	0			1	hex(13000	26	255	1	1	1
10	0	2	Mark Richi	0			1	hex(15000	26	255	1	1	1
11	0	2	Aziz Azha	0			1	hex(16000	26	255	1	1	1
12	0	2	Loretta Le	0			1	hex(19000	26	255	1	1	1
13	0	2	David Li	0			1	hex(1a000	26	255	1	1	1
14	0	2	Marcus Be	0			1	hex(1c000	26	255	1	1	1
15	0	2	Vernon Te	0			1	hex(1f000	26	255	1	1	1
16	0	2	Piere Bros	0			1	hex(20000	26	255	1	1	1

The file above is only an example of how the CSV file looks like. There are more fields than shown in the example above. For each of the field in the file saved, refer to the table below.

The following details are saved in the database:

Item	Description
Card Number	Limited to a length of 14 digits, consisting of 0 ~ 9.
Facility Code	The range of numbers for this code is dependent on the Card format used, up to a maximum of 5 digits. For example: Standard 26 bit wiegand format could have a range from 0 to 255..
Card Format-	Can be BOSCH-ADC Proprietary Card Format, Standard 26 bit Format or any other format, configurable up to a total of 16 types of card formats, including the above 2 mentioned format. '2' in the Card Format column in the exported CSV file represents the second listed card format in Access Easy Master. In this example, '2' represents 'Standard 26 bit Format', as shown below. 
User Name	Limited to a length of 30 alphanumeric characters,
Department	Configurable up to 255 departments. '0' in the Department column in the exported CSV file means that department is NOT selected for the cardholder. '1' would mean that the department is the first listed in Access Easy Master. In this example, '1' represents 'R&D Department', as shown below.
User Field 1	Limited to a length of 20 alphanumeric characters, including digits, alphabets, symbols such as # & [ ] and space. When User Field 1 is configured as 'Home Tel', the heading 'User Field 1' in the exported CSV file would appear as Home Tel. And for example, the Home Tel of Matt Brown is 67724590. In the CSV file, it will appear as shown below. 

D	E	F	G
User Name	Department	Home Tel	User Field 2
Matt Brown	0	67724590	
Krishnan	0		
Ali Ahmad	0		
Santokh Singh	0		
Lee Weng Kin	0		
Koh Buck Song	0		

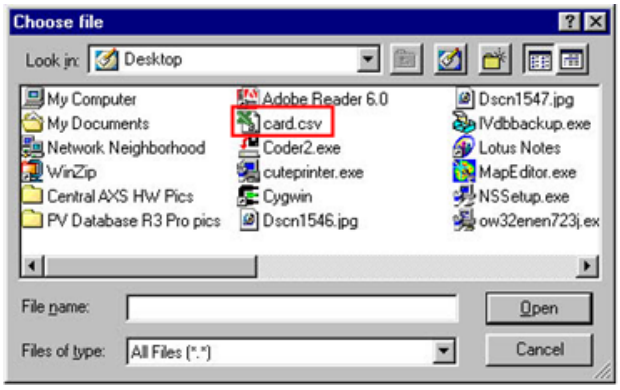
Item	Description
User Field 2	Limited to a length of 20 alphanumeric characters, including digits, alphabets, symbols such as # & [ ] and space. When User Field 2 is configured as 'Mobile', the heading 'User Field 2' in the exported CSV file would appear as Mobile. And for example, the Mobile of Matt Brown is 98904237. In the CSV file, it will appear as shown.  D / E / F / G User Name / Department / Home Tel / Mobile Matt Brown / 0 / 67724590 / 98904237 Krishnan / 0 Ali Ahmad / 0 Santokh Singh / 0 Lee Weng Kin / 0
Access Level	Can be any of the 1024 Access Level. '1' in the Access Level column in the exported CSV file means that the first Access Level is selected. '1024' means that Access Level #1024 is selected. In this example, Access Level for Matt Brown is selected as the first Access Level, as shown below.  D / E / F / G / H User Name / Depart / Home Tel / Mobile / Access Level Matt Brown / 0 / 67724590 / 98904237 / 1 Krishnan / 0 / 1 Ali Ahmad / 0 / 1 Santokh Singh / 0 / 1 Lee Weng Kin / 0 / 1 Koh Buck Song / 0 / 1
Binary	The user can leave this field blank when he is entering data in the CSV file.
Length	User has to enter the length in the CSV file. Without this field, the card will not be imported into the system. For example: For Standard 26 bit Format, the length is 26.
Arm/Disarm Zone	The number in the Arm/Disarm Zone column in the exported CSV file represents the Alarm Zone that the user can arm/disarm. The number representing the Alarm Zone is as follows:- ▶ Alarm Zone 1 - 0 - represented by 0 ▶ Alarm Zone 2 - 1 - represented by 1 ▶ Alarm Zone 3 - 2 - represented by 2 ▶ Alarm Zone 4 - 3 - represented by 3 ▶ All Alarm Zones - 5 - represented by 5 ▶ User cannot arm/disarm any alarm zone - 255
Holiday Schedule	'0' indicates that the check box *Cardholder must abide by holiday schedules* (*To work in conjunction with Reader Options*) is NOT checked. '1' indicates that the check box is checked.
Exit Sch	'0' indicates that the check box for A*llow exit reader usage only in accordance with time schedules* is NOT checked. '1' indicates that the check box is checked.

Item	Description
Enable Enroll	'0' indicates that the check box for *new enrolment for the reader schedules* is NOT checked. '1' indicates that the check box is checked.
One Time Access	'0' indicates that the check box *Cardholder with one time access only* is NOT checked. '1' indicates that the check box is checked.
Card + PIN	'0' indicates that the check box for *Card + PIN is required on keypad readers* in Access Easy Master is NOT checked. '1' indicates that the check box is checked.
Extended	The number in the Extended column indicates the extended duration for Door Strike and Keypad Timeout. For example, '0' indicates that there is no extended duration for Door Strike and Keypad Timeout. '10' indicates that there is an extended duration of 10 seconds for Door Strike and Keypad Timeout for the cardholder.
Start Date	'0' indicates that the check box for *Start Date* in Access Easy Master is NOT checked. '1' indicates that the check box is checked.
Year	The number in this Year column in the exported CSV file represents the year for the Start Date for the card to take effect.
Month	The number in this Month column in the exported CSV file represents the month for the Start Date for the card to take effect.
Day	The number in this Day column in the exported CSV file represents the day for the Start Date for the card to take effect.
End Date	'0' indicates that the check box for *End Date* in Access Easy Master is NOT checked. '1' indicates that the check box is checked.
Year	The number in this Year column in the exported CSV file represents the year for the End Date for the card to cease being effective.
Month	The number in this Month column in the exported CSV file represents the month for the End Date for the card to cease being effective.
Day	The number in this Day column in the exported CSV file represents the day for the End Date for the card to cease being effective.
Dual Card Assignment	'0' indicates that the radio button for *Dual Card not assigned* is selected. '1' indicates that the radio button for *Dual Card presentation sequence is selected.*
Dual Card Presentation Sequence	'0' indicates that 'First Card' is selected for *Dual Card presentation sequence*, '1' indicates that 'Second Card' is selected and '2' indicates that 'Don't Care' is selected
Group ID	The number in the Dual Card Group ID column indicates the group ID the card falls into.
Card Pin	The number in the Card Pin column indicated the encrypted card pin number. Default card pin number is set at 1234000.
Card Disabled	'0' indicates that user card is NOT disabled for access, '1' indicates user card is disabled from all access to the system permanently.

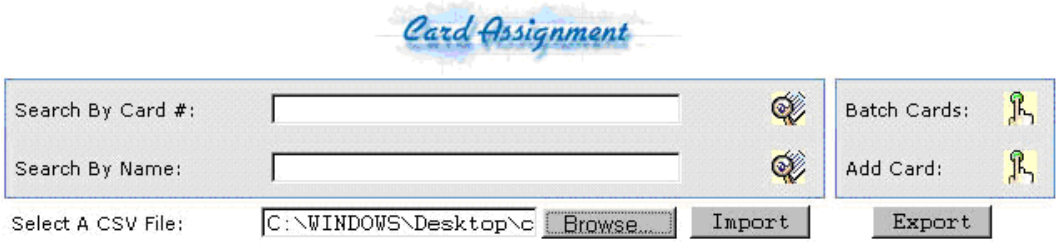
6.3.2 How to Import the Card Database

Sometimes, user may have a lot of changes to make or new cards to add before importing the card database into the system.

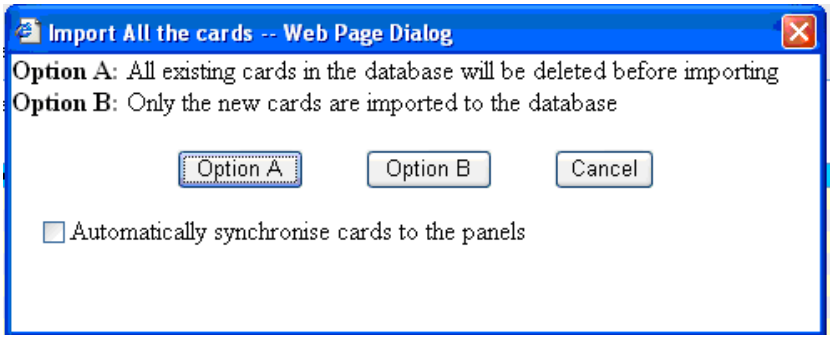
1. To import card database into the system, select a file to be imported by clicking on the Browse... button. The *Choose File* dialogue box will appear for the user to choose the file to be imported, as shown below.



2. Select the file in CSV format to be imported to the system and click the [Open] button.
3. The file name and directory will appear in the space provided beside *Select a CSV File*, as shown below.



4. Click on the Import button to import the card database into the system. The box as shown below will appear.


Import All the cards -- Web Page Dialog
Option A: All existing cards in the database will be deleted before importing
Option B: Only the new cards are imported to the database
Option A
Option B
Cancel
Automatically synchronise cards to the panels

5. There are 2 options that user can choose from.

Options	Description
Option A	When this option is selected, the existing database will be deleted before the new database are imported.
Option B	When this option is selected, only the new cards are imported to the database
Cancel	Cancel the import function.

NOTICE!
If you wish to synchronise the new database to all the controllers, please check the box first before selecting your desired option.

6. The card database will be imported into the system.

6.3.3 Cards Enrolment Operation

This function is to facilitate selected card holders to have the right to use their card to activate a Reader to be in enrolment mode.

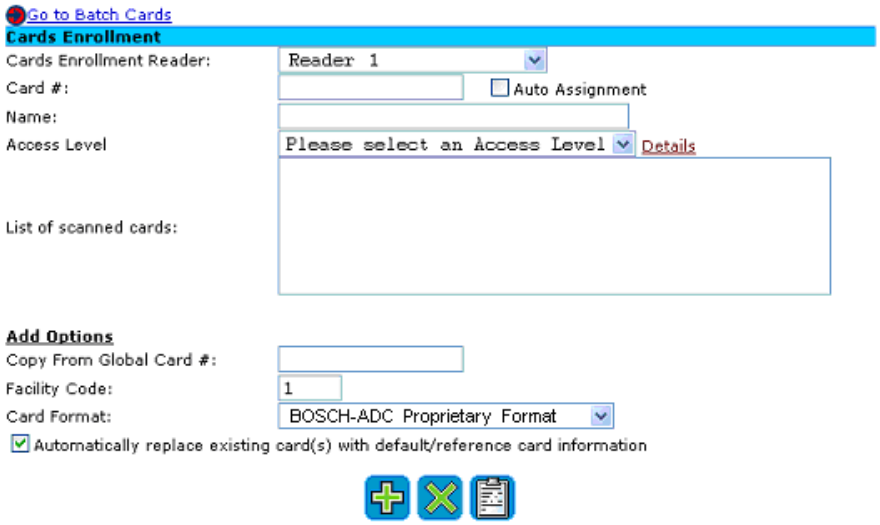
6.3.4 Card Enrolment of Card with Unknown Wiegand Format

To use any unknown proprietary wiegand card format, administrator can activate a Reader, either by pre-assigned enrolment card or by web page, to be in enrolment mode and enrol any card into the card database (maximum bit length is 64).The sections below will guide the administrator on how to activate a Reader to be in enrolment mode, both by enrolment card and by web page.

Card Enrolment Using Web Page

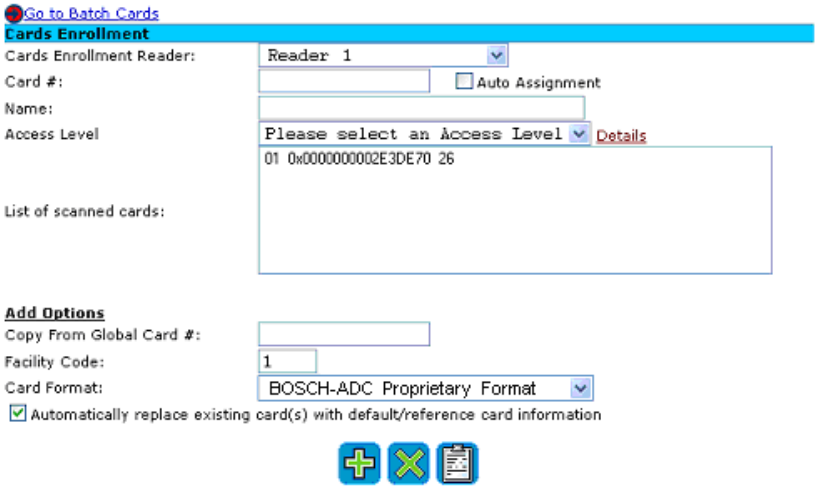
If the administrator chooses to enrol a card of unknown proprietary wiegand card format using the web page, he should follow the steps below.

1. To go to the page as shown below, select *Card Assignment* from the Left Pane, followed by *Batch Cards* Batch Cards: at the top-right corner, and lastly select *Go to Cards Enrolment* Go to Cards Enrollment. The screen as shown below will appear.



Select a Reader to be the enrolment Reader. In this example, we select Reader 1 to be the enrolment Reader.

2. Click on the button to activate the selected Reader as the enrolment Reader.
3. Present the card with unknown Wiegand Format to the enrolment Reader, which is Reader 1 in this example. The card that has been presented to the enrolment Reader will appear in the box for *List of scanned cards*, as shown in the screen below.

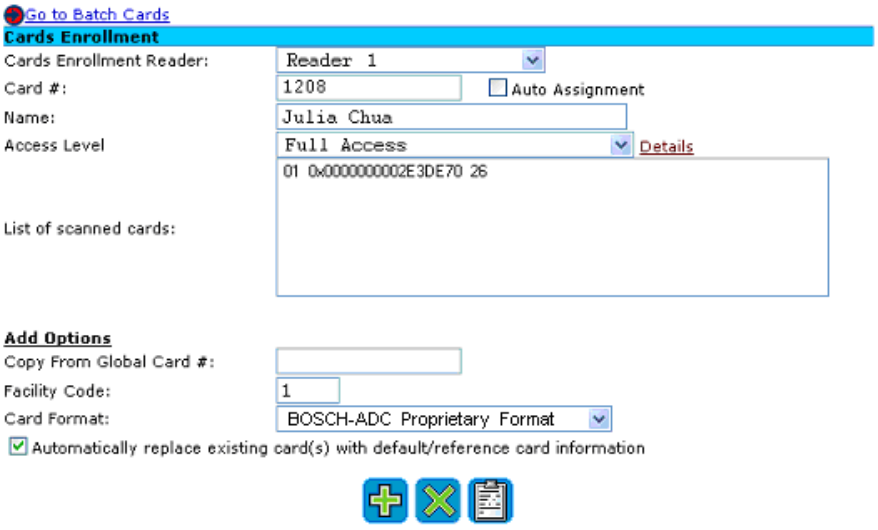


4. The administrator can now assign any Card #, Name and Access Level to the card. In the screen below, the Card # is assigned as 1208, the Name of the cardholder as Julia Chua and the Access Level as Full Access, Refer to *Chapter 7 Access Levels for more details*.

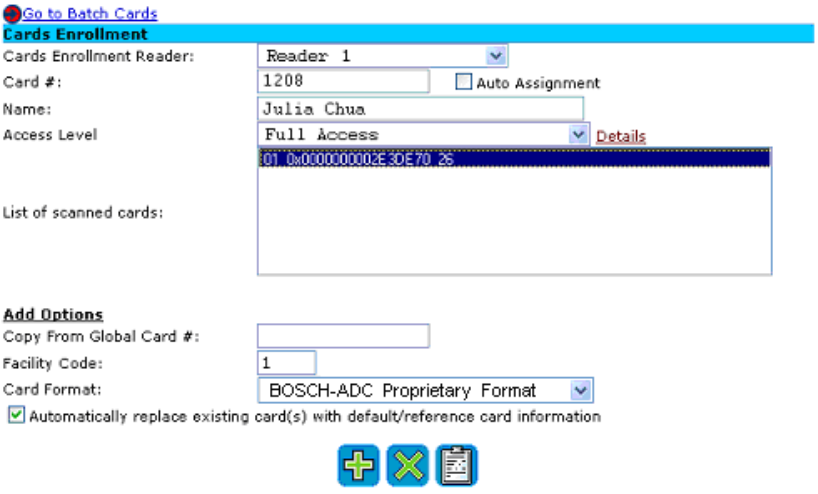
NOTICE!

If you have a number of cards to enrol, for example 20 cards. You can select Auto Assignment feature which will automatically increment the Card number after you enrol the first card.

It is recommended that the administrator assigns a number to the card of unknown wiegand format beforehand and sticks a label on the card, so that it is easier to refer to the card number during the card enrolment process.



5. Highlight the card in the *List of scanned cards* that you are assigning the Card # and Name to, as shown in the screen below.



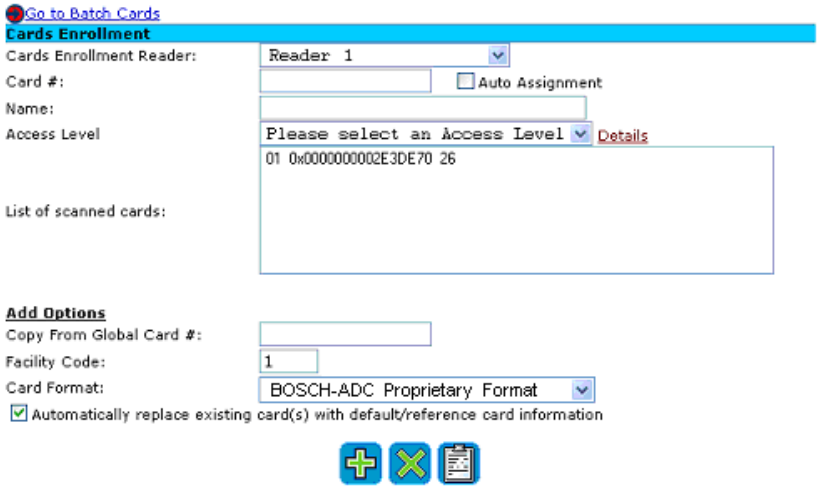
6. Click on the button to add the card with the assigned Card # and Name to the database.

Card Enrolment Using Pre-Assigned Enrolment Card

A pre-assigned enrolment card is a user card that has been checked with the option Card Holder Can Enable Enrolment Operation. For the details on how to set a card to be a pre-assigned enrolment card, refer to the section *Card Holder Can Enable Enrolment Operation above*.

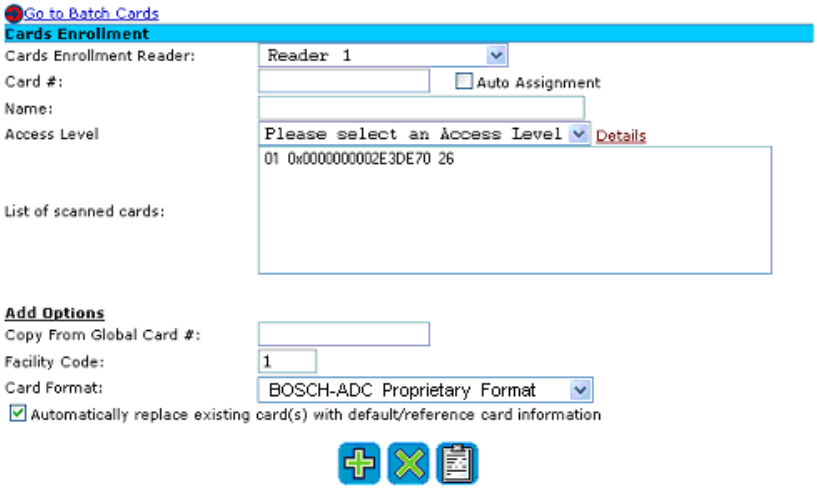
If the administrator chooses to enrol a card of unknown proprietary wiegand card format using pre-assigned enrolment card, he should follow the steps below.

1. To go to the page as shown below, select Card Assignment from the Left Pane, followed by Batch Cards Batch Cards: at the top-right corner, and lastly select *Go to Cards Enrolment* Go to Cards Enrollment .The screen as shown below will appear.



2. Present the pre-assigned enrolment card to a Reader. The Reader is now activated to be in enrolment mode. If the pre-assigned enrolment card also has access right to the Reader, press key <7> on the Keypad before presenting the pre-assigned enrolment card.
3. Present the card with unknown Wiegand Format to the enrolment Reader. If key <7> is pressed before presenting the pre-assigned enrolment card, the timing on Keypad Time-out will have to be observed. This means that when a pre-assigned enrolment card is presented to the Reader to activate the Reader as an enrolment Reader, the new card to be added to the panel has to be presented to the same Reader within the timing set in Keypad Timeout. Failure to do so will cause the Reader to return to normal mode. For the setting of timing on the Keypad Timeout, please refer to *Chapter 16 Panels Admin, Card Readers, Keypad Timeout*.

   The card that has been presented to the enrolment Reader will appear in the box for *List of scanned cards,* as shown in the screen below.



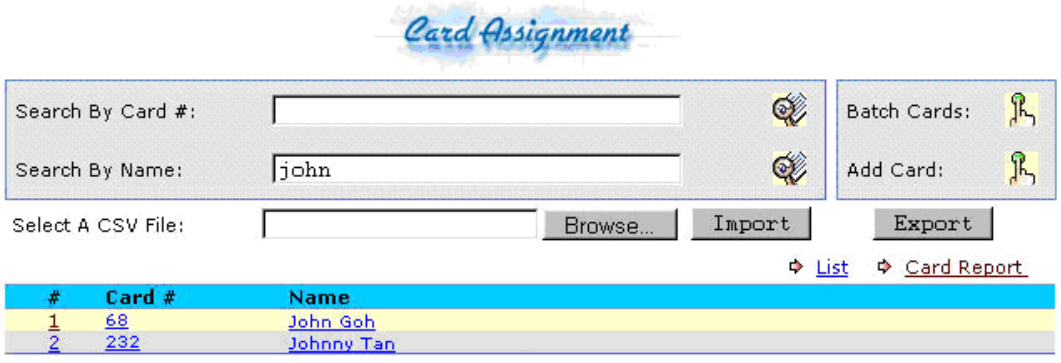
4. To add in the new card to the card database, refer to *Steps 5 ~ 6* in the section *Card Enrolment Using Web Page above*.

6.4 How to Use Search Function

The Card Assignment menu allows us to search for cards by name or by card number.

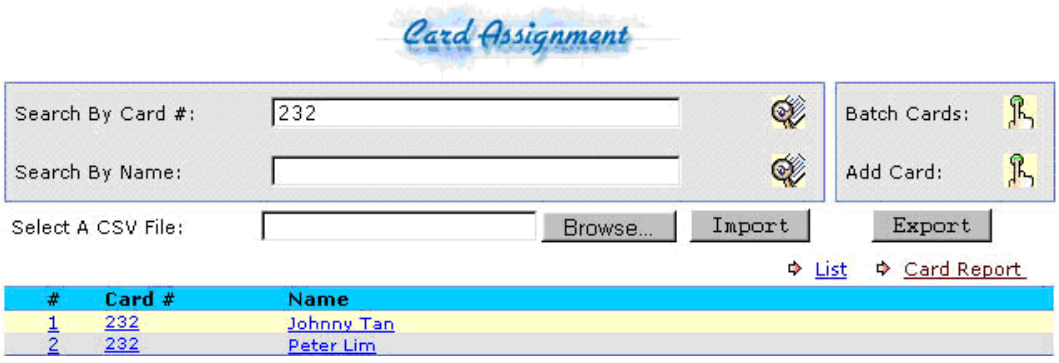
If you want to search by card number, you may enter the card number in the *Search By Card #* field. If you want to *search by user name*, enter the user name in the Search By Name field.

Let us consider an example. Suppose we want to search for a cardholder named John. The resultant screen will be as follows.



Searching for a cardholder named John will display all users with John in their names. You can directly click on the user to go to the user details page.

Let us consider another example. Suppose we want to search for a Card Number 232. The resultant screen will show Card information of the search, as shown on the following page.



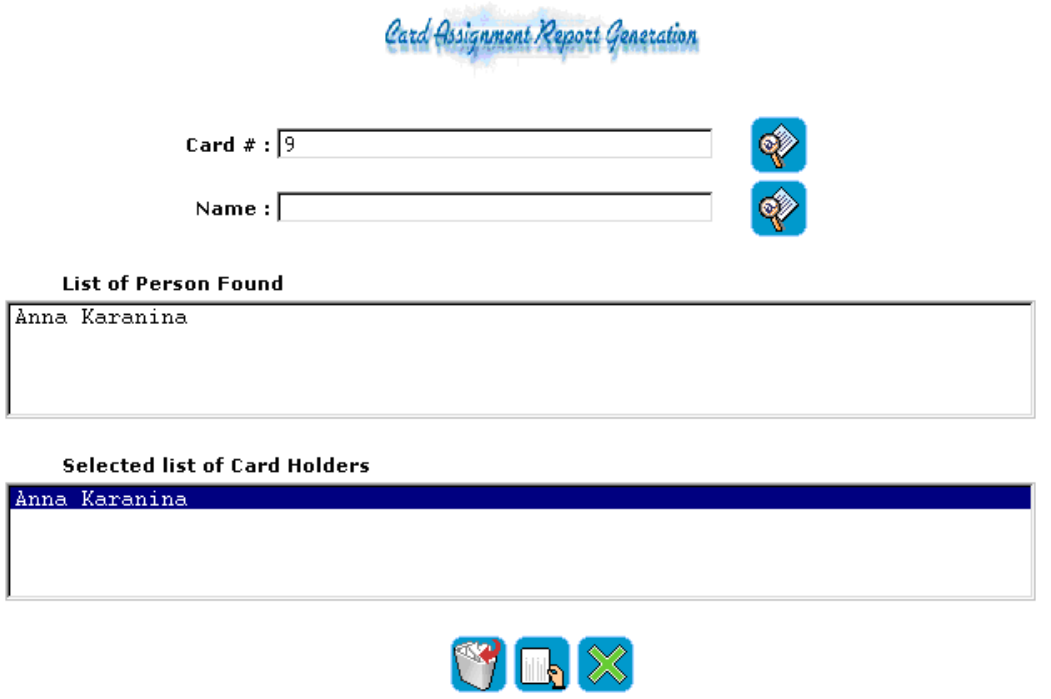
Searching for a card with card number 232 will display all cards with card number 232. If the system has two or more cards with exactly the same card number, but their Card Format or Facility Code is different, a list of User names will be listed for your selection.

6.5 How to Generate Card Assignment Report

The Card Assignment Report Generation feature allows us to view a report on all or selected cardholders based on their Name or their Card Number.

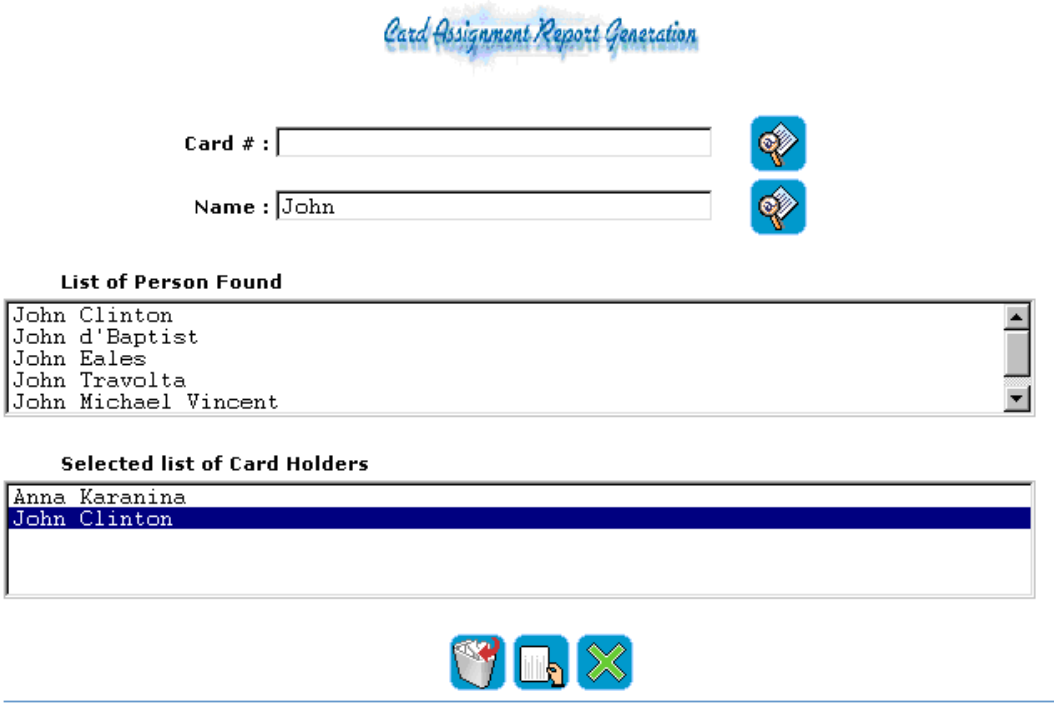
When we select on the Card Report hyperlink Card Report on the first page of Card Assignment, we will see a screen as shown below.

We may either search for a cardholder by Card Number or by Name and add to the selected list of cardholders. When we perform a search by Card Number, you will see a screen as shown below. Let us assume that we are searching for a card number 9.



When we search for a card number 9 (for example), you will see a screen as above. We will be able to see the Name of the person corresponding to the Card Number. Clicking once on the person's name will add that person to the *Selected list of Card Holders*.

We may also perform a search by Name. Let us consider, for example, that we are searching for a Name 'John'. When we perform a search for John, we will be able to see all persons having 'John' in their name.



We may select the person you want to add to the *Selected list of Card Holders* by clicking once on the person's name in the *List of Person Found* window.

To generate a cardholders report based on the parameters above, click on the submit icon.

A sample report is shown below.

Bosch Security Systems Pte Ltd
30C Jalan Pemimpin Singapore 577180

Card Assignment Report
Thursday, 11 Sep 2003 12:40:44

Legends

Arm/Disarm	*- Card holder is able to Arm/Disarm*
Holiday Sch	*- Card holder must abide by holiday schedules (To work in conjunction with Reader Options)*
Exit Sch	*- Allow exit reader usage only in accordance with time schedules*
Card + PIN	*- Card + PIN is required on keypad readers*
Enable Enroll	*- Card holder can enable enrollment operation*
One Time Access	*- Card holder with one time access only*
Extended	*- Extended duration for door access*

#	Card # / Facility Code / Department / Enable Enroll / Panel Description	Name / Access Level / Card Type / One Time Access	Card Format / User Field 1 / User Field 2 / Dual Card Assignment / Access Group A	Arm/Disarm / Holiday Sch / Exit Sch / Card + PIN / Access Group B	Start Date / End Date / Extended
1	9	Anna Karanina	Standard 26 bit Format	Not Selected	11 Sep 2003
	0	Full Access Level		Selected	----
	Sales & Marketing	Global		Selected	0 seconds
	Not Selected	Not Selected	Not Assigned	Selected	
2	402	John Clinton		Not Selected	11 Mar 2003
	0	Full Access Level		Selected	----
	Engineering	Global		Selected	0 seconds
	Not Selected	Not Selected	Not Assigned	Selected	

Page 1 of 1

It contains all the details found under the *Card Details* and *Card Functionality*.

7 Access Levels

An *Access Level* is defined as a group of Access Groups, while an *Access Group* defines a list of readers within certain authorised time periods (pre-defined *Schedule*) that the cardholders can access. There are 1024 programmable Access Levels.

In addition, there are two more unique access levels. They are the Full Access level that allows cardholders to access all readers at all times, usually reserved for the President, Chairman or Directors of the company and the *Unused* level that prohibits cardholder to access any reader at all times.

Access Level is implemented to simplify the process of assigning cardholder's access rights to each reader in each Access Easy Controller. In a system where more than one Access Easy Controller are implemented to control the access of doors, we will need to configure the cardholder number into each and every one of the Access Easy Controller. This is a very time consuming process. With Access Easy Master, we could configure cards for the cardholders by assigning them Access Levels. Each Access Level could define the Access Groups that the cardholder belongs to in each Access Easy Controller.

It is highly recommended that detail planning be done before setting up the *Access Levels*.

7.1 The Access Levels page

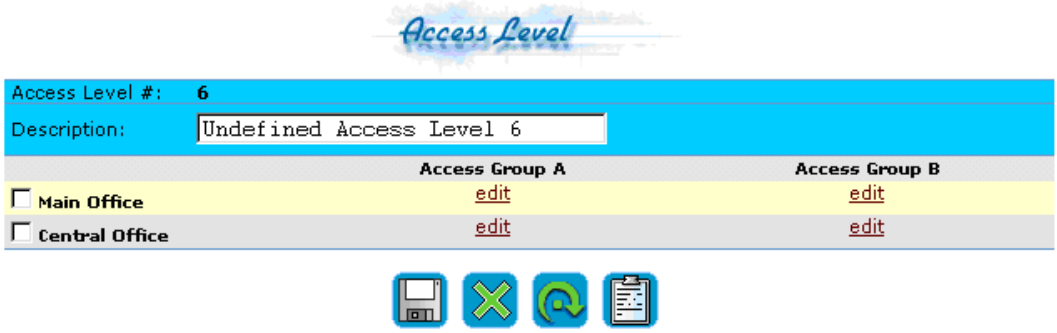
To activate Access Levels, click on Access Levels hyperlink from the main menu page. The Access Levels screen will appear as shown below.

Access Level
1 – 100
Access Level Report
Access Level #
Description
1 Full Access Level
2 Director and President Access
3 Managers Access
4 Staff Access
5 Visitor Access
6 Undefined Access Level 6
7 Undefined Access Level 7
8 Undefined Access Level 8
9 Undefined Access Level 9
10 Undefined Access Level 10
11 Undefined Access Level 11
12 Undefined Access Level 12
13 Undefined Access Level 13
14 Undefined Access Level 14
Click on any of the Description or Access Level # to configure the Access Level

The *Access Levels* screen will show the different Access Levels with their descriptions. After activating the Access Levels, we need to configure the Access Levels for granting access across different Controllers. Select from the list box on the top left corner to select Access Level # that are more than 100.

7.2 How to Configure Access Levels

1. Click on the Access Level (*can be any of the 1024 undefined Access Levels)* you want to configure. You will see a screen as shown below.



2. Enter the *Description* for the Access Level in the space provided.
3. You will see a list of available Access Easy Controllers in the Access Level screen.
4. Check on the Controllers you wish to add in the Access Level. For this example, the controller is Central Office .
5. Click on the *edit* hyperlink under *Access Group A* or *B* to select the appropriate Access Grouping for *Access Group A* and *B* from the list. There is no priority or precedents in *Access Group A* or *B*. When any of the *edit* hyperlink is clicked for that row, the screen as shown below appears.

6. Click on the down arrow to select an Access Group for *Access Group A* and *Access Group B*. Leave the entry as blank or *Unused* if it is not required.

7. Click to save the new settings.

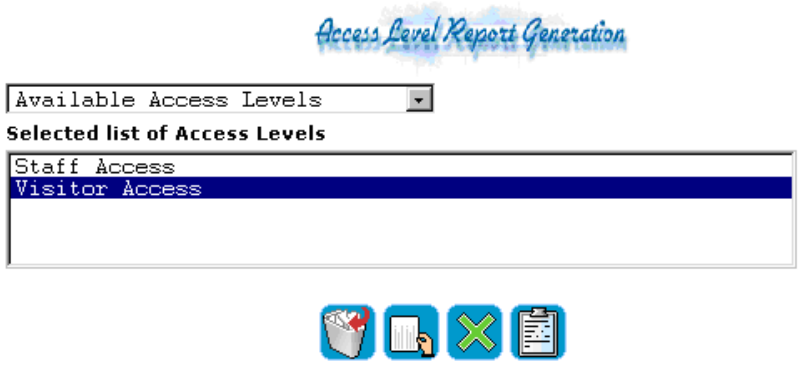
NOTICE!
The Access Groups in each controller has to be pre-defined in the controller itself. To define the Access Groups in the individual controller, go to Panels Admin, Access Groups.

7.3 How to Print Access Level Report

An *Access Level* report contains details of all the *Access Levels* which are configured. Undefined Access Levels will not be included in the report.

To print an Access Level Report, click on Access Level Report located on the top right corner of the Access Levels first page.

The *Access Level Report Generation* web page has a drop down list box which shows all the configured Access Levels. Select the Access Levels you want to include in the Access Level Report by clicking once on the Access Level in the drop down box. The *Selected List of Access Levels* window will display the Access Levels you want to be included in the Access Level Report.



NOTICE!
Only configured Access Levels will be shown in the list box for selection. Configured Access Levels are those with at least one Access Easy Controller checked and at least one Access Group configured and not left blank.

To print an Access Level Report, click on the submit icon.

A sample Access Level Report is as shown below.

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Access Level Report
Wednesday, Aug-25-2004 3:08:34:AM

Access Level # / Panel Description	Access Level Description / Access Group A	Access Group B
1	**Roaming Access for Science Pk**	
Central Office	Full Access	Unused
Gateway Office	Full Access	Unused
2	**Level 2 Managers Access**	
Central Office	Normal Access Group	Unused
Gateway Office	Normal Access Group	Unused
3	**Level 1 Managers Access**	
Central Office	Unused	Normal Access Group

8 Users Setup

Each user can be assigned access rights to access and carry out configuration on certain or all functions of the Access Easy Master. Access Easy Master can support up to 25 users, including the super user whose access rights cannot be changed.

The *Users Setup* menu item allows the System Administrator to define different access to users, by selecting whether a particular user can have *View* and/or *Save* rights to configuration functions.

It is important that only authorized users are able to change the following settings, as the implication could be a security breach, if unauthorized user gives themselves access to important feature in the system, such as full access for their cards or unlock a door.

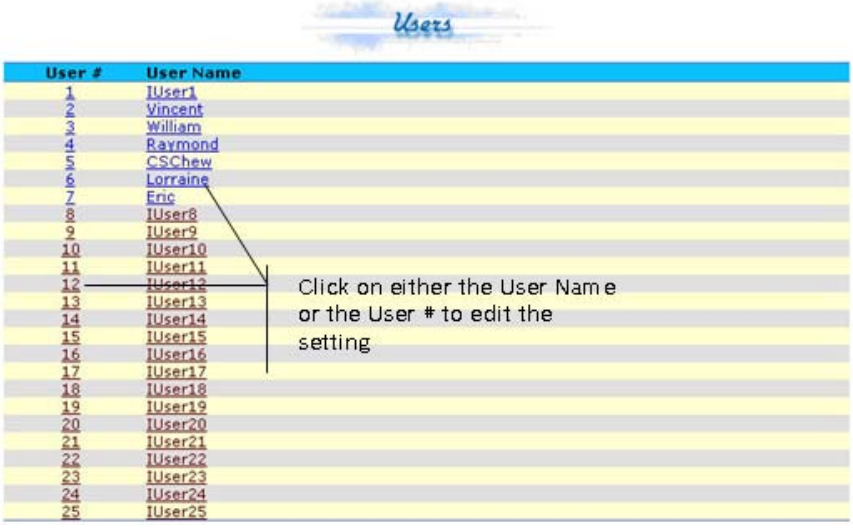
NOTICE!
The default Password and User ID should be changed once the system is in operation!

In the following sections of this Chapter, we will be referring to *Login User* as the user who will login to the Access Easy Master from any computer using a Web Browser program and operates the system.

8.1 Setting User Access

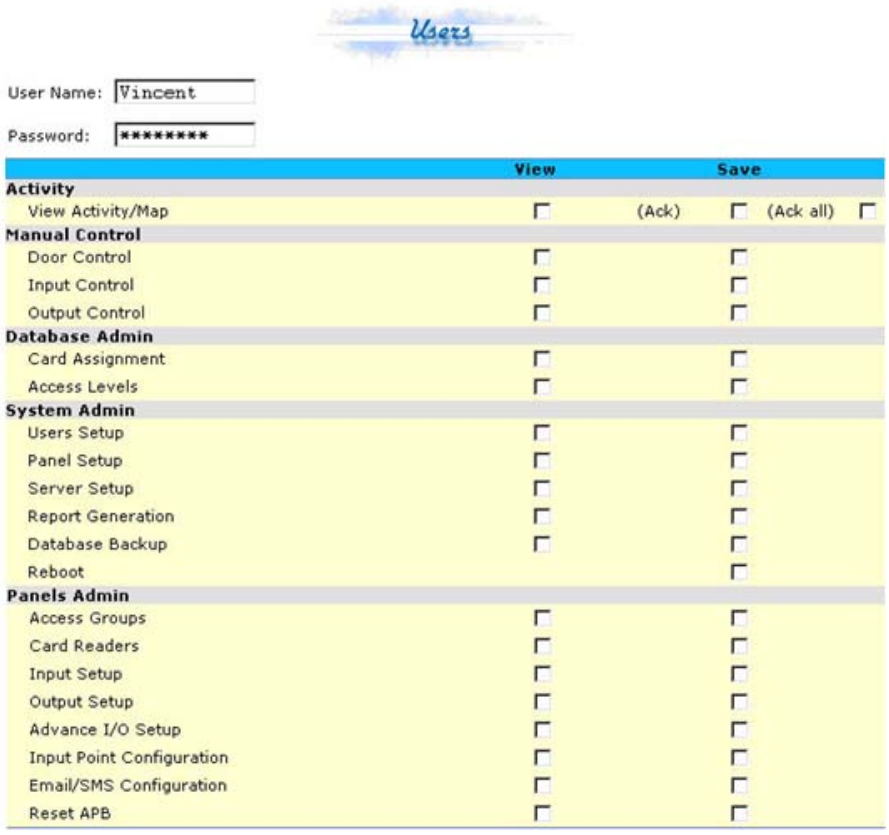
This section describes how to change User Name and Password and how to change the access to menu items.

The following is a screen of the *Users Setup* page.



8.1.1 How to Change User Name and Password

1. Click on the User Name or its User # and the following screen will appear.



NOTICE!

The first Login User will always be the Super User. A Super User has access to all menu items and its settings cannot be changed except for the User Name and the Password.

Check box that are grey out like this ☑ indicates that the setting cannot be changed.

2. To edit the User Name, delete the default User Name and enter the new User Name, limiting to eight alphanumerical characters including punctuation marks.

3. To edit the Password, delete the default Password and enter the new Password, limiting to eight alphanumerical characters (see Notice below).

NOTICE!

The Password is case-sensitive.

For security reason, every character entered for the Password is represented by an asterisk . For Macintosh user, it is represented by a dot instead.

4. Click on the icon to save the settings. The new settings will only take effect upon the next successful login.

8.1.2 How to Change the Access to Menu Items

View
Refers to having the right to access and view the contents of the menu item.

Save
Refers to having the right to access and edit the contents of the menu item.
When only the Save function for the menu item is checked, the system would treat that both *View* and *Save* function is enabled.

1. To assign the various menu item access rights, check the checkbox of the desired menu item under *View* and/or *Save* column. To de-select the point, click on it again.

2. Click on the icon to save the settings. The new settings will only take effect upon the next successful login.

9 Panel Setup

This Chapter will provide a step by step guide to how to add an Access Easy Controller.

The *Panel Setup* allows us to identify the Access Easy Controller that will be managed by the Access Easy Master. It will also show the connection status of the Access Easy Controller with the Access Easy Master.

Below is a screen of the *Panel Setup*.

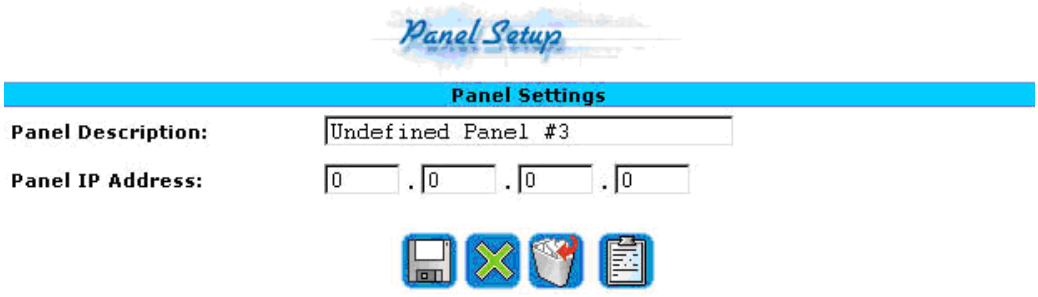
Panel #	Panel Description	Status
1	Central Office	Connected
2	Gateway Office	Connected
3	Undefined Panel #3	Not Setup
4	Undefined Panel #4	Not Setup
5	Undefined Panel #5	Not Setup
6	Undefined Panel #6	Not Setup
7	Undefined Panel #7	Not Setup
8	Undefined Panel #8	Not Setup
9	Undefined Panel #9	Not Setup
10	Undefined Panel #10	Not Setup
11	Undefined Panel #11	Not Setup
12	Undefined Panel #12	Not Setup
13	Undefined Panel #13	Not Setup
14	Undefined Panel #14	Not Setup
15	Undefined Panel #15	Not Setup
16	Undefined Panel #16	Not Setup
17	Undefined Panel #17	Not Setup
18	Undefined Panel #18	Not Setup
19	Undefined Panel #19	Not Setup
20	Undefined Panel #20	Not Setup

The maximum number of Access Easy Controller that Access Easy Master can support is 20.

9.1 How to Add an Access Easy Controller

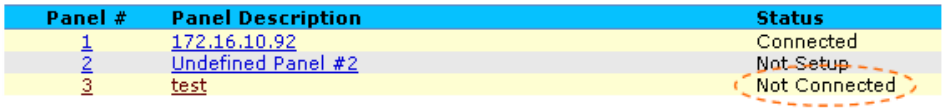
Before the user proceeds with the following steps, he should ensure that the Access Easy Master IP Address is also registered in the Access Easy Controller. To register the Access Easy Master IP Address in the Access Easy Controller, log in to the Access Easy Controller itself to register.

1. Click on any of the undefined controller (in this example, Panel #3 is not configured yet) and the following screen will appear.



2. Enter the Controller description and the Controller IP Address. Click on the icon to save your settings. To delete a Controller, click on the icon.

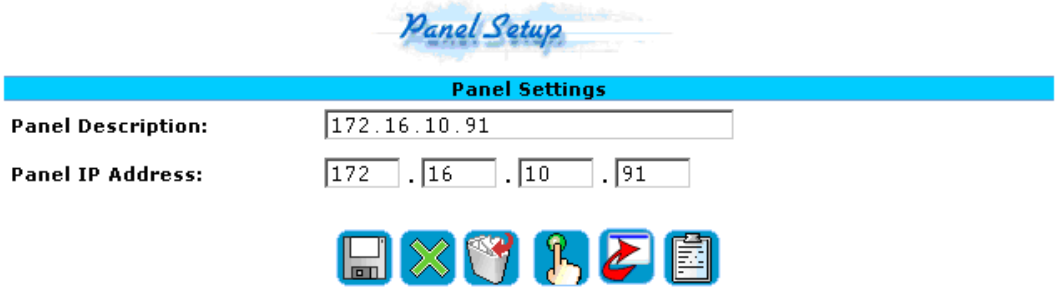
3. Once the IP address of the new Access Easy Controller has been added to the *Panel Setup* page, Access Easy Master will attempt to connect to the new controller and synchronize the database. If Access Easy Master fails to connect to Access Easy controller, status will show not connected.



The Status column shows the status of the Access Easy Controllers with respect to the Access Easy Master.

Status	Indicates
Not Connected	Access Easy Master is unable to detect the Access Easy Controller
Initialising	Access Easy Master is synchronizing with the Access Easy Controller. This will only happen when a new Controller is added and new database has to be created
Deleting	Access Easy Master is deleting the database. This will only happen when a Controller is deleted.
Connected	Access Easy Master is able to detect the Access Easy Controller.
Not Setup	There is no Access Easy Controller setup.

4. After the Controller is successfully connected to the Server, there will be 2 extra button and in the Panel Settings, as shown below, for the user to synchronize the following data and settings configured in the Access Easy Master to the Controller: *Card Database, Holidays, Schedules* and the groups under Controllers Admin such as *Access Groups, Card Readers, Input Setup, Output Setup, Advance I/O Setup, Input Point Configuration* and *Email/SMS Configuration*.



9.1.1 How to download database to controller

User can download database to the controller, this allows user more control to select desired controller to update the database. This feature is useful if some controllers in the system are not fully operational and the user does not wish to update these controllers yet. Or a faulty controller is being replaced with a new one, hence the user could use this feature to download the database back to the new controller.

NOTICE!
Access Easy Master can only download database to controller with status "Connected"

Download database to controller

1. Click on the desired controller.
2. Click on the icon download the database.
3. Click on OK to start overwrite the existing database of the selected controller.
4. Once the new database is downloaded Click on the icon to return.

NOTICE!

The following database will be downloaded to the controller, *Card Assignment, Access Level, Holidays, Schedule, Department List, Access Group, Card Readers, Input Setup, Output Setup, Advance I/O Setup, Input Point Configuration* and *Email/SMS Configuration* database.

Download card database to controller

1. Click on the desired controller.
2. Click on the icon download the card database.
3. Click on OK to start overwrite the existing card database of the selected controller.
4. Once the new card database is downloaded. Click on the icon to return.

NOTICE!

Only Card database will be downloaded to the controller.

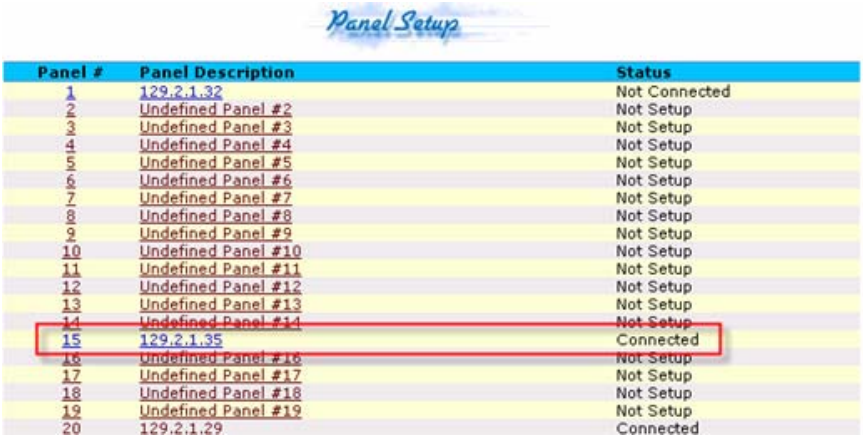
9.2 How to download database to Panel

User can download database to the controller, this allows user more control to select desired controller to update the database. This feature is useful if some controllers in the system are not fully operational and the user does not wish to update these controllers yet. Or a faulty controller is been replace with a new one, hence the user could use this feature to download the database back to the new controller.

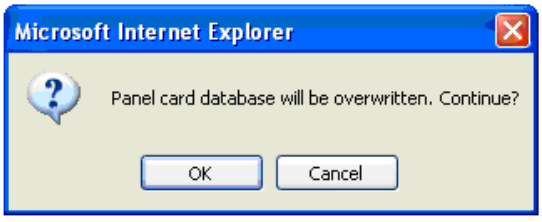
NOTICE!

Only controllers with the status "Connected" are able to download any new database to the controller

1. Click on the desired controller (in this example, Panel #15 selected.


Panel Setup
Panel #
Panel Description
Status
1 129.2.1.32 Not Connected
2 Undefined Panel #2 Not Setup
3 Undefined Panel #3 Not Setup
4 Undefined Panel #4 Not Setup
5 Undefined Panel #5 Not Setup
6 Undefined Panel #6 Not Setup
7 Undefined Panel #7 Not Setup
8 Undefined Panel #8 Not Setup
9 Undefined Panel #9 Not Setup
10 Undefined Panel #10 Not Setup
11 Undefined Panel #11 Not Setup
12 Undefined Panel #12 Not Setup
13 Undefined Panel #13 Not Setup
14 Undefined Panel #14 Not Setup
15 129.2.1.35 Connected
16 Undefined Panel #16 Not Setup
17 Undefined Panel #17 Not Setup
18 Undefined Panel #18 Not Setup
19 Undefined Panel #19 Not Setup
20 129.2.1.29 Connected

2. Click on the icon download the database.
3. Click on OK to start overwrite the existing database of the selected controller.



4. Once the new database is downloaded. Click on the icon to return.

10 Holidays

Holidays are holidays that are applicable to all the Access Easy Controllers managed by the Access Easy Master. Holidays have to be set up only if the system operation behaviour is required to be different during holidays. Some samples of how the parameters affect the system operation behaviour are: -

- The Controller unlocks a specific door during certain working hours of the day. However, during a holiday, the door will remain locked the whole day.
- A cardholder is allowed access to certain areas during working hours. However, during a holiday, the cardholder is not allowed access.

By providing a centralized configuration of holidays, the Server Administrator can just configure Holidays in the Access Easy Master and it will synchronize with all the Access Easy Controllers automatically.

This section covers the step-by-step guide to set up *Holidays* parameters.

Holidays set-up consist of 64 Holidays selection, of which 32 are assigned to *Regular Holiday* dates and the other 32 assigned to *Special Holiday dates*. There is no difference between the operational behaviour of both types. For simplicity, you may treat the *Special Holiday* set up for use during the eve of a holiday.

Each Holiday # has the feature *Include year in processing?*. If it is set to No, the Controller will not consider the Year during a date check. This is very useful if the holiday date falls on the same date year after year, e.g. *New Year day* and *Christmas Day* need to be defined only once. While those holiday dates that vary from year to year will have to be updated at the beginning of the year, and shall be selected to *Yes*.

User can use this feature to ease the updating of holiday dates every year by allocating, for example, the first 10 Holiday # for fixed holiday dates and the rest of the Holiday # for variable holiday dates. In this way, user just has to update on the variable holiday dates and skip the fixed holiday dates at the beginning of the year.

10.1 How to configure Holidays

1. From the Left Pane menu, select *Holidays*. A screen as shown below appears.

Global Holidays
Regular Holidays
Special Holidays
Holidays Report
Regular Holiday #
Description
1 New Year Day
2 Lunar New Year
3 Christmas Day
4 Undefined Regular Holiday 4
5 Undefined Regular Holiday 5
6 Undefined Regular Holiday 6
7 Undefined Regular Holiday 7
8 Undefined Regular Holiday 8
9 Undefined Regular Holiday 9
10 Undefined Regular Holiday 10
11 Undefined Regular Holiday 11
12 Undefined Regular Holiday 12
13 Undefined Regular Holiday 13
14 Undefined Regular Holiday 14
15 Undefined Regular Holiday 15
16 Undefined Regular Holiday 16
17 Undefined Regular Holiday 17
18 Undefined Regular Holiday 18
19 Undefined Regular Holiday 19
20 Undefined Regular Holiday 20
Click on either the Holiday # or Description to configure

2. Click on the Regular Holidays or Special Holidays link to list the appropriate holiday type.
3. Click on the *Holiday #* or the *Description* text to proceed. A screen as shown below appears.

Global Holidays
Regular Holidays
Regular Holiday # : 4
Holiday Description: Undefined Regular Holiday 4
Current Holiday Date:
New Holiday Date: Day: Month: Year:
Include year in processing? Yes No

4. Delete the default text and enter the new *Holiday Description*.
5. Select the New Holiday Date from the list box, for the *Day, Month* and *Year*. After it is selected and saved, it will reflect on the *Current Holiday Date*.
6. If the Holiday date is fixed, then click on the radio button of the *Include year in processing?* to *No*, otherwise click *Yes*.
7. Do one of the following: -

- To confirm the entries, click on the button. This will cause the Access Easy Master to start replicating the changes to the rest of the Access Easy Controllers.
- To clear the entries, click on the button.
- To cancel the operation, click on the button.
- To return to the first page, click on the button.

8. Proceed to configure other Holiday dates where applicable.

The example below shows selection of *Regular Holiday* #1 used for *Christmas* in the year 2004. Since the date always fall on the December 25th, the *Include year in processing?* was set to *No*.

10.2 How to Generate a Holidays Report

Once you have completed configuring the required Holidays, a hardcopy can be printed out. To print any one or all Holidays (Regular or Special) configuration, follow the steps below.

1. From the first page of either the *Regular* or *Special Holidays*, click on the link
   Holidays Report . The example below shows the Regular Holidays Report generation.

2. Select the desired Holiday from the list box and it will appear on the *Selected list of Holidays* box, as shown below. If no Holiday is selected from the list, all the available Holidays with date settings will be included in the report.

3. To remove the selected holiday from the Selected list of Holidays, select that holiday and click on the button.
4. Click on the button for a print preview of the report.

The following screen-capture shows an example of the Regular Holidays Report

NOTICE!
Only Holiday # with date setting will be shown.

Bosch Security Systems Pte Ltd
30C Jalan Pemimpin Singapore 577180

Regular Holidays Report
Thursday, Aug-26-2004 2:58:23:PM

#	Description	Date
1	New Year Day	Jan-01-
2	Lunar New Year	Feb-15-2004
3	Christmas Day	Dec-25-

11 Schedules

Schedules can be used in the following manner:

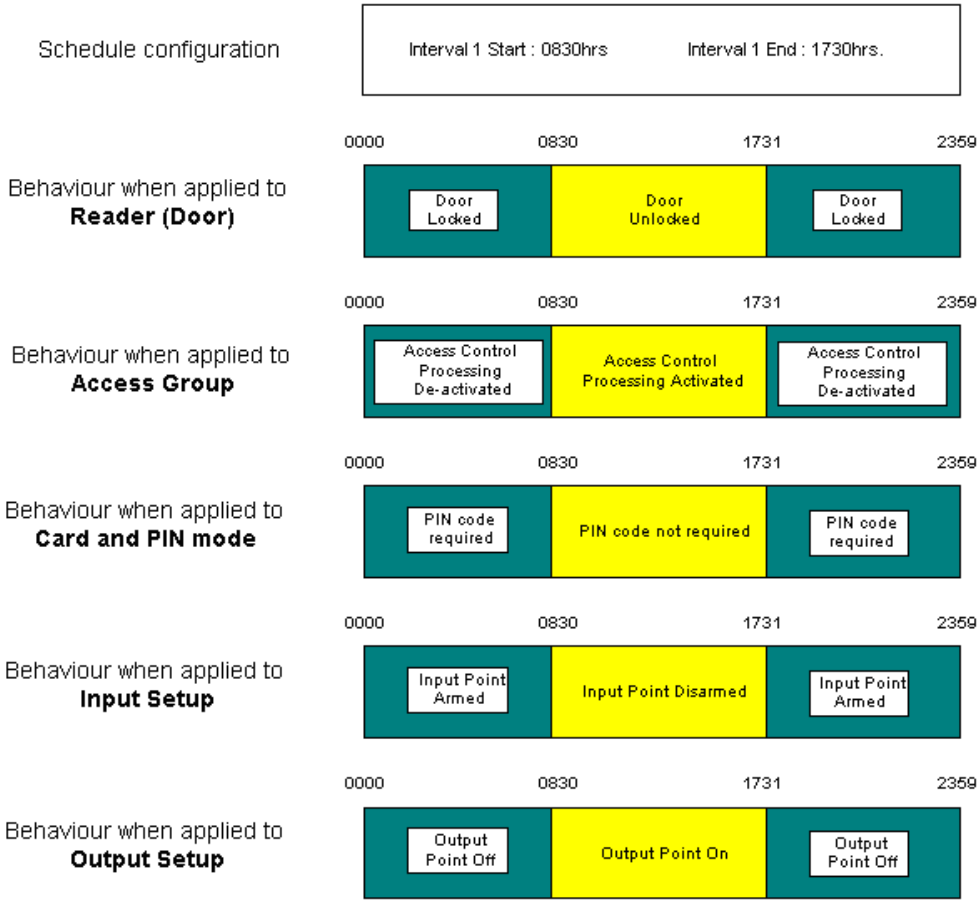
- Schedules are allocated to Card Readers for Access Groupings. This is to specify whether cardholders can access specific readers at specific time or cardholders need to enter PIN at specific time.
- Schedules are allocated to the Card Readers to activate or deactivate readers at specified time. It is also used to define whether PIN mode will be used for the reader at specified time.
- It is used to define the time intervals to Arm / Disarm Alarm Zone.
- It is used to define the time intervals for triggering of the Output Points. For example, this is used for scheduled triggering of lighting utility for an area.

Schedules are common to all the Access Easy Controllers managed by the Access Easy Master.

NOTICE!
All entries for time are based on 24-hour, 4-digits format.

11.1 System Behaviour when using Schedule

The diagram below provides a graphical representation of the system's behaviour when a Schedule is used on the various functions.

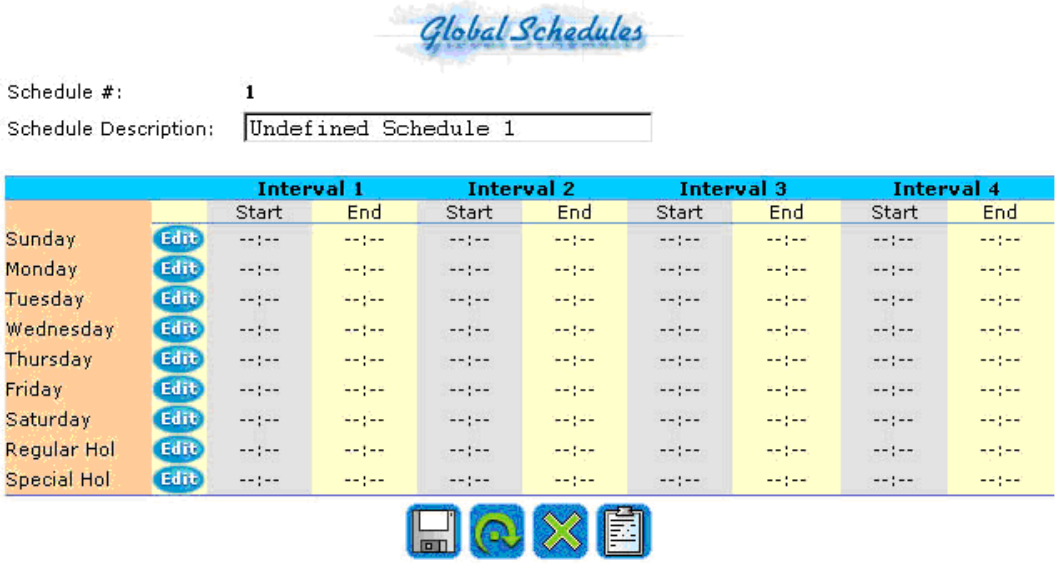


Notice that all the functions toggle its state only at 1731hrs instead of 1730hrs. The reason is that Access Easy Controller takes 17:30:59hrs as a valid End time for 1730hrs.

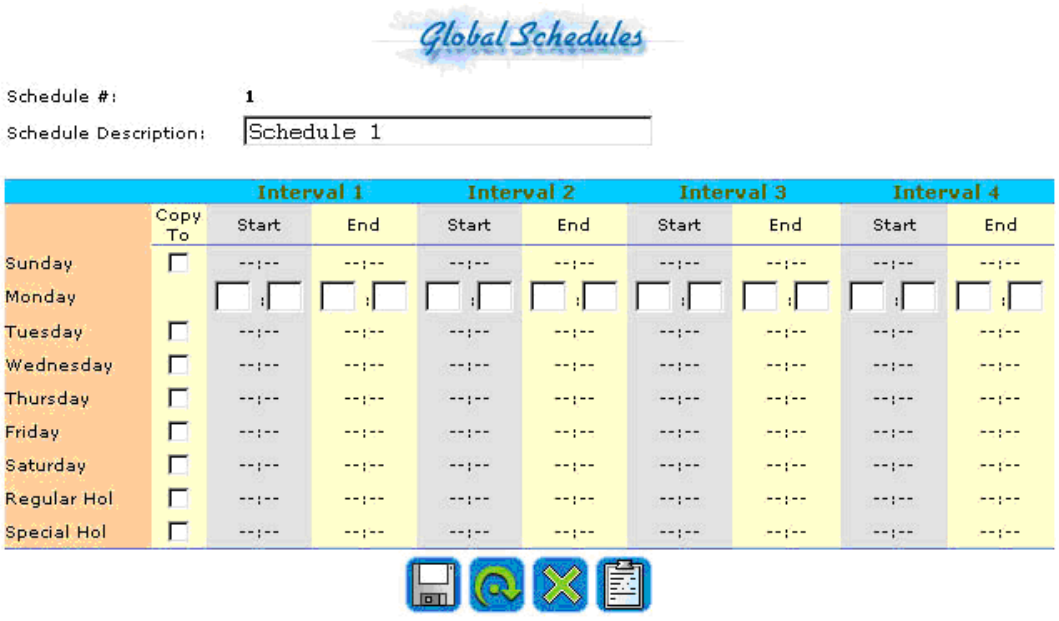
11.2 How to Configure Schedules

1. From the Left Pane menu, select *Schedules*. A screen as shown below appears.

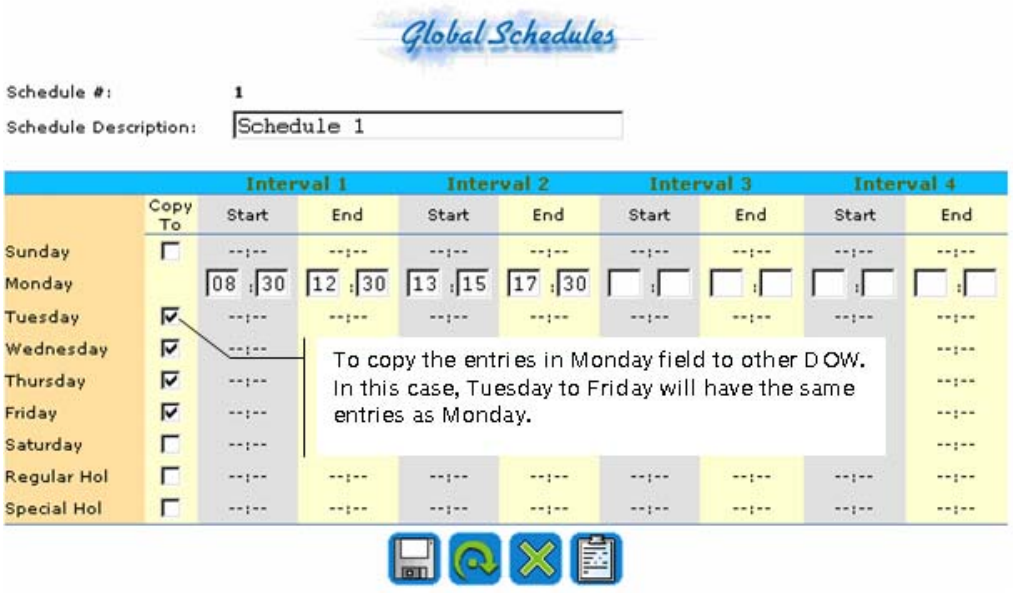
2. Click on the 1-128 or 129-255 link to list the appropriate Schedule range.
3. Click on the *Schedule #* or the *Description* text to proceed. A screen as shown below appears.



4. Delete the default text and enter the *Schedule Description*.
5. Click on the button.
6. Click on the button of the Day of Week (DOW), *Regular Hol* or *Special Hol* row. This will enable the whole row for editing as shown on the following page.



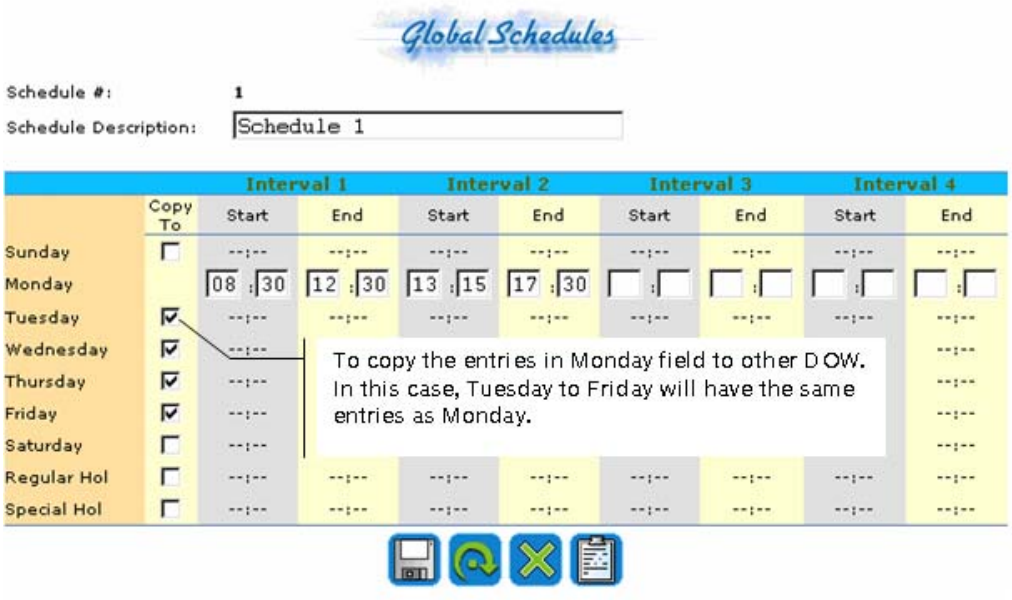
7. Click on the required field, starting from Interval 1 - Start, and enter the appropriate time



in 24-hour, 4 digits format.

8. Repeat step 7 until all applicable entries are entered.

9. If the time of operation is the same for Monday to Friday, click on the Copy To check boxes to indicate a tick mark. This will duplicate the setting to other DOW, Regular Hol or Special Hol, as shown below. To de-select the *DOW*, click on it again.



10. Do one of the following: -

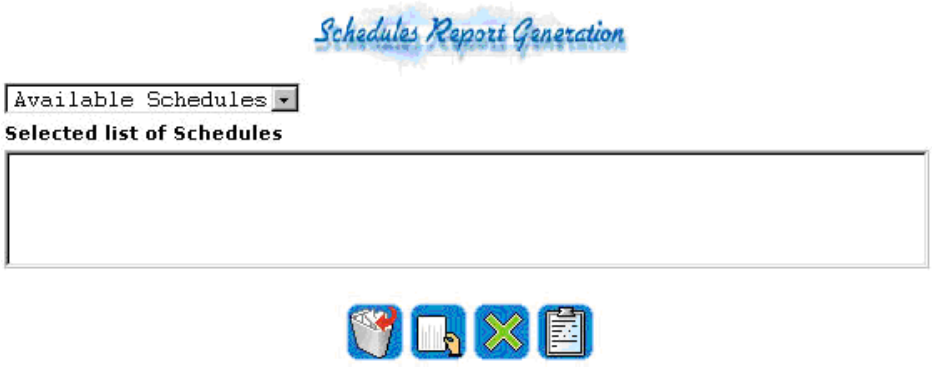
- To confirm the entries, click on the button. This will cause the Access Easy Master to replicate the Schedule to the rest of the Access Easy Controller.
- To clear the entries, click on the button.
- To cancel the operation, click on the button.
- To return to the first page, click on the button.

11. Proceed to edit the other *DOW* or *Holiday* where applicable. If the company does not operate during Sunday or Holiday, leave the entries in these 3 fields unchanged as -- : --. This will indicate to the Controller that these are to be ignored.

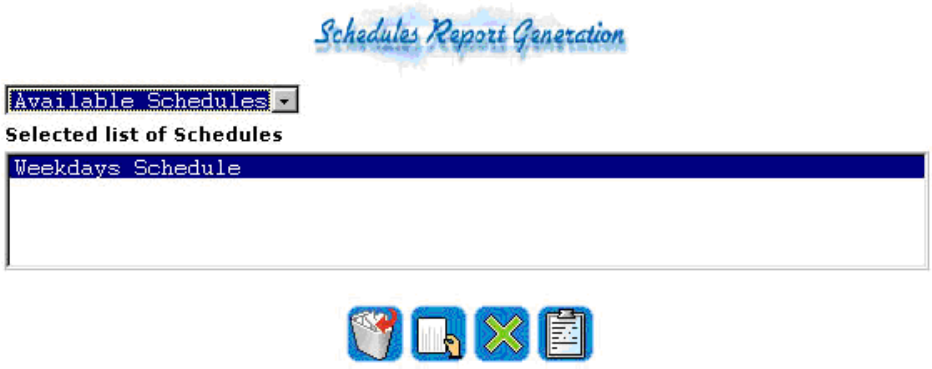
11.3 How to Generate a Schedule Report

Once you have completed configuring the required Schedules, a hardcopy can be printed out.

1. From the first page of the Schedules, click on the link Schedules Report . A screen as shown on the following page.



2. Select the desired Schedule from the list and it will appear on the *Selected list of Schedules box*, as shown below. If no Schedule is selected from the list, all the available Schedules with time settings will be included in the report.



3. To remove the selected schedule from the Selected list of Schedules, select that schedule and click on the button

4. Click on the button for a print preview of the report.

The following screen-capture shows an example of the Schedules Report.

NOTICE!
Only Schedule # with time setting will be shown.

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Schedules Report
Thursday, Aug-26-2004 4:13:54:PM

#	Description	Day	Interval 1 Start	Interval 1 End	Interval 2 Start	Interval 2 End	Interval 3 Start	Interval 3 End	Interval 4 Start	Interval 4 End
1	Weekdays Schedule									
		Sun	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
		Mon	08:30	12:30	13:15	17:30	--:--	--:--	--:--	--:--
		Tue	08:30	12:30	13:15	17:30	--:--	--:--	--:--	--:--
		Wed	08:30	12:30	13:15	17:30	--:--	--:--	--:--	--:--
		Thu	08:30	12:30	13:15	17:30	--:--	--:--	--:--	--:--

12 Server Setup

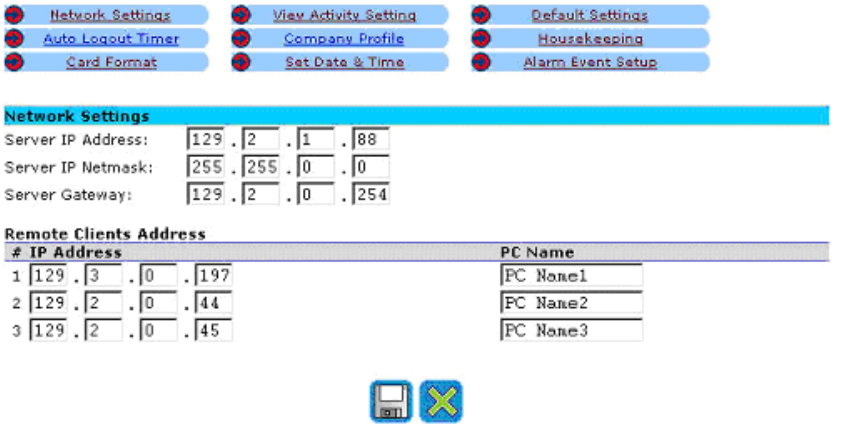
Server Setup involves setting up the Access Easy Master and configuring its various parameters.

These parameter includes: -

- Network Settings,
- Auto Logout Timer,
- Card Format,
- View Activity Setting,
- Company Profile,
- Set Date and Time,
- Default Settings,
- Housekeeping,
- Alarm Event Setup.

12.1 Network Settings

Network settings involve configuring the various network parameters for Access Easy Master such as IP address, subnet mask and gateway. It also involves setting up the Remote Clients IP address. Click on Network Settings from the menu item list and you will see a screen as shown below.


Network Settings
Auto Logout Timer
Card Format
View Activity Setting
Company Profile
Set Date & Time
Default Settings
Housekeeping
Alarm Event Setup
Network Settings
Server IP Address: 129 . 2 . 1 . 88
Server IP Netmask: 255 . 255 . 0 . 0
Server Gateway: 129 . 2 . 0 . 254
Remote Clients Address
IP Address
PC Name
1 129 . 3 . 0 . 197
PC Name1
2 129 . 2 . 0 . 44
PC Name2
3 129 . 2 . 0 . 45
PC Name3

This configuration allows user to enter the *Server IP Address, Server IP Netmask* and *Server Gateway*. In addition, user can define 3 *Remote Clients Address* for ftp (file transfer protocol) purposes.

12.1.1 How to Edit Network Settings

1. Delete the default number in each of the *Server IP Address, Server IP Netmask* and *Server Gateway* field and enter the appropriate number.
2. Click on the icon to save the settings (see NOTICE).

NOTICE!
In order for the new IP Address to take effect, the Access Easy Master needs rebooting.

12.2 Auto Logout Timer

This configuration allows user to set the timer for the Access Easy Master software to *Logout* automatically if it detects no user activity. Default setting is 1 hour. Click on *Auto Logout Timer* from the menu item list and you will see a screen as shown below.

NOTICE!
This Timer setting is applicable to all menu items except *View Activity*.

12.2.1 How to set the Auto Logout Timer

1. Select the *Hour* and *Minute* from the list box.
2. Click on the icon to save your setting. Click on the icon to clear the setting.

12.3 Card Format

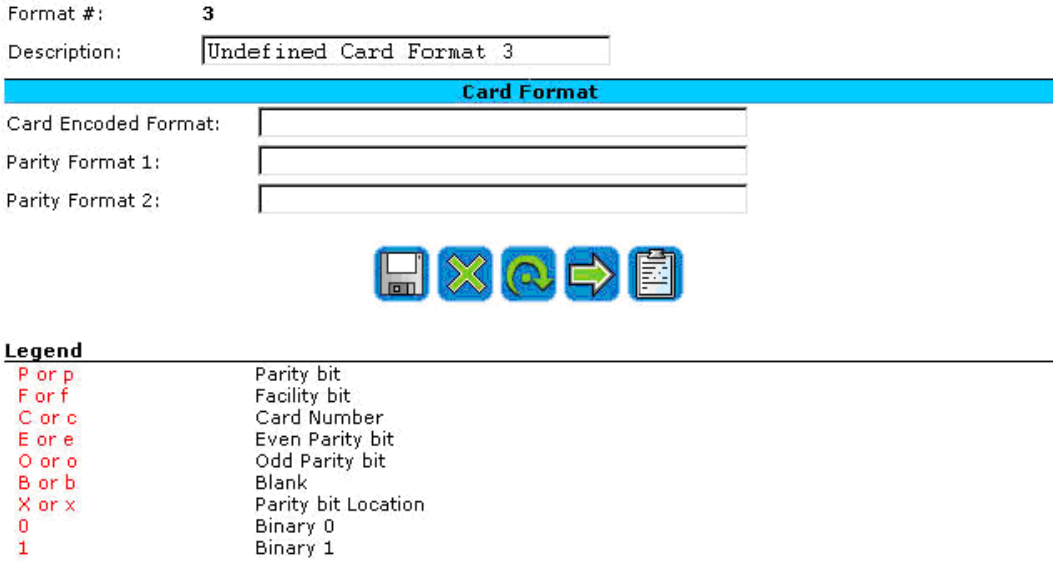
This setting allows user to customise the Access Easy Master to accept up to 16 different types of Wiegand card format, inclusive of the BOSCH-ADC Proprietary Card Format and the standard AEC Priority Format, which have been pre-assigned to Format #1 and #16 respectively. Card Format up to a maximum of 64-Bit and up to 8 Parity Format is configurable. Click on *Card Format* from the menu item list and you will see a screen as shown below.

Network Settings | Input Point Configuration | Set Date & Time
Auto Logout Timer | Audit Log | Default Settings
Card Format | Company Profile | Email/SMS Configuration

Format #	Description
1	BOSCH-ADC Proprietary Format
2	Standard 26-bit Card Format
3	Standard 34-bit Card Format
4	Undefined Card Format 4
5	Undefined Card Format 5
6	Undefined Card Format 6
7	Undefined Card Format 7
8	Undefined Card Format 8
9	Undefined Card Format 9
10	Undefined Card Format 10
11	Undefined Card Format 11
12	Undefined Card Format 12
13	Undefined Card Format 13
14	Undefined Card Format 14
15	Undefined Card Format 15
16	AEC Priority Format

12.3.1 How to Configure New Card Format

1. Click on the *Format #* or *Description* text of any Undefined Card Format to proceed. A screen as shown below appears.



2. Delete the default text and enter a *Description* for this *Card Format*.
3. Enter the card format for the *Card Encoded Format* field accordingly.
4. Enter the parity for *Parity Format 1* and *Parity Format 2* (please apply the condition in NOTICE 1 here and for subsequent Parity Format fields).

NOTICE!

1. The entries to this field must not contain Parity Bit Location that depends on the resultant Parity Bit of the next or higher (Parity Format 2 to 8) Parity Format field entries.

2. If the Card Format doesn't support Parity checking, leave the All Parity Format fields blank.

In order to understand how to configure the different format, the standard 26-Bit Wiegand card format will be used as an example.

Example: 26-Bit Wiegand Card Format

The 26-bits of transmission from the Reader to the Access Easy Controller consists of two parity bits and 24 code bits. The first transmitted bit is the Even parity bit E and it is calculated over the first 12 bits. The last bit transmitted is the Odd parity O and it is calculated over the last 12 bits.

The string of bits for this code format is shown in the following tables. Due to the lack of space, the 26-Bits is split into two separate rows of 13 each.

Code Format

1	2	3	4	5	6	7	8	9	10	11	12	13
E	F	F	F	F	F	F	F	F	C	C	C	C

14	15	16	17	18	19	20	21	22	23	24	25	26
C	C	C	C	C	C	C	C	C	C	C	C	O

Legend:
E: Resultant Even Parity Bit
F: Facility Code Bit
C: Card Number Bit
O: Resultant Odd Parity Bit

Parity Format

1	2	3	4	5	6	7	8	9	10	11	12	13
P	E	E	E	E	E	E	E	E	E	E	E	E

14	15	16	17	18	19	20	21	22	23	24	25	26
O	O	O	O	O	O	O	O	O	O	O	O	P

Legend:
E: Even Parity Bit Location
P: Resultant Even and Odd Parity Bit
O: Odd Parity Bit Location

In order for the Access Easy Controller to decode the data string correctly, we need to configure the code accordingly.

Referring to the Code Format Table

1. Enter P or p for the resultant Even (E) and Odd (O) Parity Bit
2. Enter F or f for the Facility Code Bit (F)
3. Enter C or c for the Card Number Bit (C)

Referring to the Code Format Table

1. Enter P or p for the resultant Even (E) and Odd (O) Parity Bit
2. Enter F or f for the Facility Code Bit (F)
3. Enter C or c for the Card Number Bit (C)

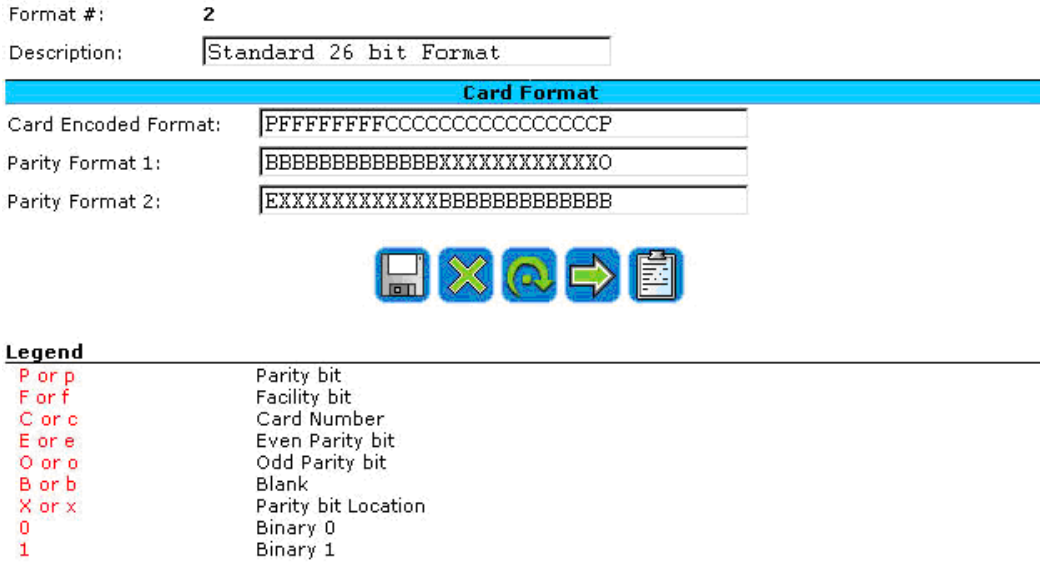
Referring to the Parity Format Table
For the Odd Parity Format.

1. Enter O or o for the resultant Odd Parity Bit (O)
2. Enter X or x for Odd Parity Bit Location.
3. Enter B or b otherwise.

For the Even Parity Format.

1. Enter E or e for the resultant Even Parity Bit (E)
2. Enter X or x for Even Parity Bit Location.
3. Enter B or b otherwise.

With the information, proceed to configure the Card Format as shown below.


Format #: 2
Description: Standard 26 bit Format
Card Format
Card Encoded Format: PFFFFFFFFCCCCCCCCCCCCCCCCP
Parity Format 1: BBBBBBBBBBBBBXXXXXXXXXXXXO
Parity Format 2: EXXXXXXXXXXXXBBBBBBBBBBBBB
Legend
P or p Parity bit
F or f Facility bit
C or c Card Number
E or e Even Parity bit
O or o Odd Parity bit
B or b Blank
X or x Parity bit Location
0 Binary 0
1 Binary 1

If you have Card Format that has more than 2 Parity Format (maximum is 8), click on the button to configure them else just save the configuration.

TIP:To best distinguish between the alphabet "O" and the number "0", it is recommended that you use all lower case entry.

12.4 View Activity Setting

This setting affects the number of transaction records to view on screen for the *View Activity* menu. However, should there be alarms that are not acknowledged by the user, the View Activity records will expand to show all transactions from the first "not acknowledged" alarm up to the latest transaction. In simple words, the View Activity is dynamic and will show those "not acknowledged" Alarm transactions up to the latest transactions.

The number of records to view ranges from 10 to 70 in steps of 10 records. Click on *View Activity Setting* from the menu item list and you will see a screen as shown below.

12.4.1 How to Edit View Activity Setting

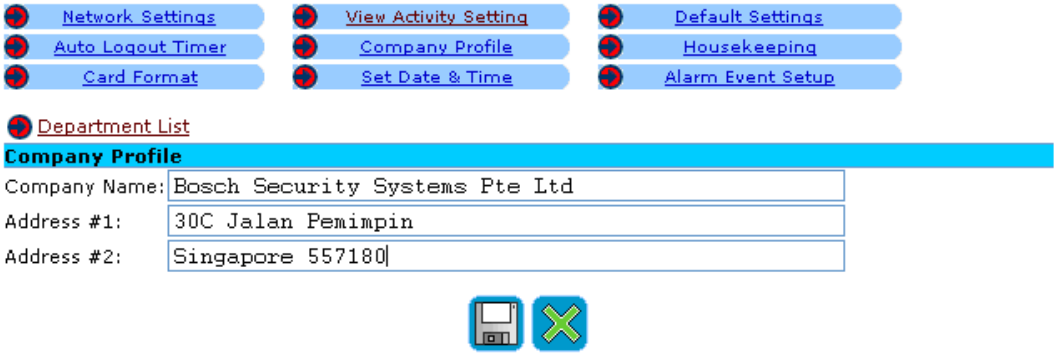
1. Select the appropriate number from the *Number of Transactions To View* list box.
2. Click on the icon to save your setting.

12.5 Company Profile

The Company Profile feature is used as a letterhead in all the report generated as shown below:-

- Card Report,
- Access Level Report,
- Holidays Report,
- Schedules Report,
- Audit Log Report,
- Access Groups Report,
- Card Reader Report,
- Input Point Report,
- Output Point Report and
- Advance I/O Report.

Each field is limited to a 50-characters entry, including punctuation. In this section, user can also configure the departments available in the company. Click on *Company Profile* from the menu item list and you will see a screen as shown below.



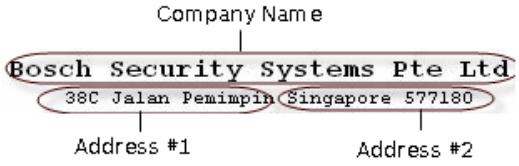
12.5.1 How to Edit Company Profile

1. Delete the default text and enter the desired Company Name.
2. Do likewise for the Address #1 and Address #2 field.
3. Click on the button.

As an example, we enter the following information in the respective fields:

Company Name: Bosch Security Systems Pte Ltd
Address #1 : 30C Jalan Pemimpin
Address #2 : Singapore 577180

For the information entered above, the letterhead will appear as shown below. Notice that *Address #1* and *Address #2* is automatically separated by a comma.

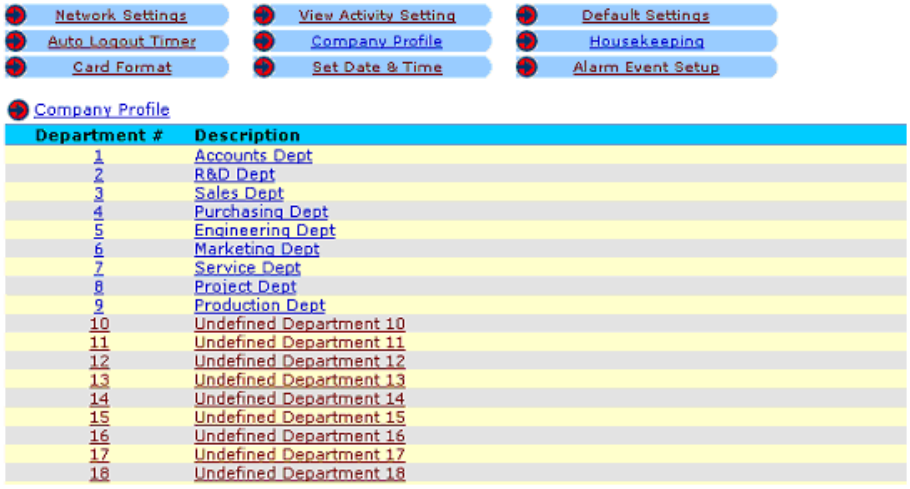


12.5.2 How to Edit the Department List

User can configure the departments available in the company in the Department List. User can then select the department that the cardholders belong to when doing card assignment. Please refer to *Chapter 5 Card Assignment, The Card Parameters, Card Details, Department* for the assignment of departments to cardholders.
To edit the Department List, follow the steps below:-

1. From the Company Profile main page as shown below, click on the Department List link.

2. The screen as shown below appears.



3. Click on any *undefined Department #* or its *Description* to configure a new department. The screen as shown below appears.

4. Enter a description for the department and click on the button.

12.6 Set Date & Time

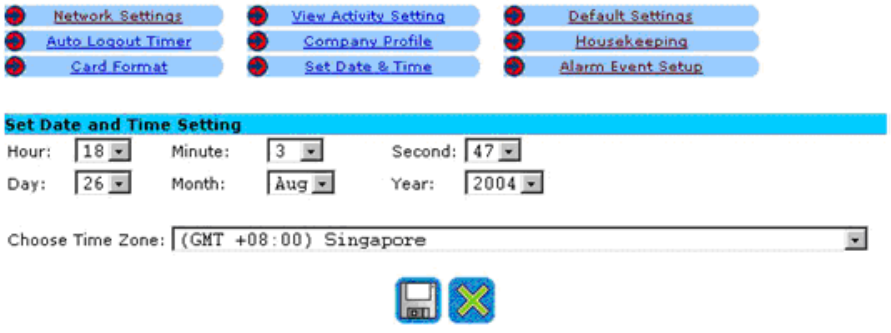
The Access Easy Master software allows user to set the date and time of the real-time clock within the Server. When the date and time is set in the Server, the date and time is synchronized to the Controller. User can also choose the Time Zone in which the Server is operating in.

On the other hand, the Controller can have a different Time Zone from the Server if the Controller is operating in another Time Zone. The time from the Server would be synchronized to the Controller accordingly.

Time setting is in the 24-hour format.

Click on *Set Date & Time* from the menu item list and you will see a screen as shown below.

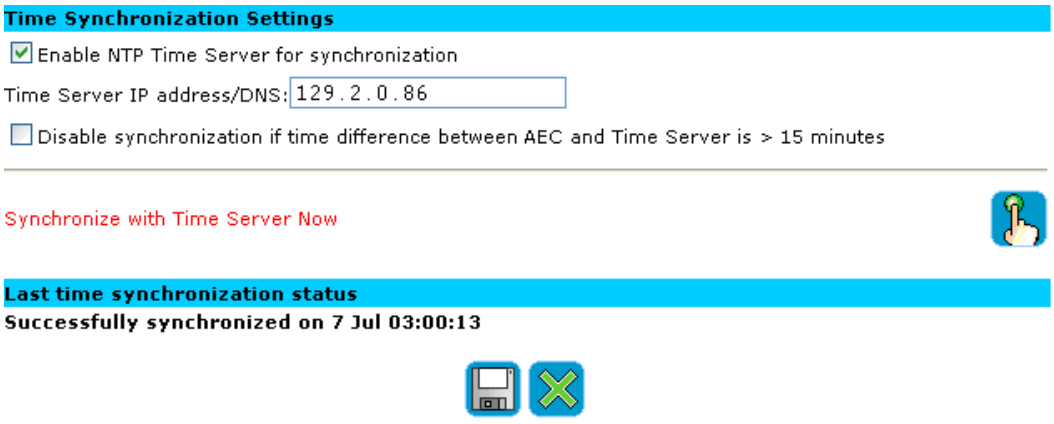
NOTICE!
For the transactions in View Activity, transactions from Panel #1 will send the date and time of the activities that have taken place to the Server and the Server will convert the time according to the Server's Time Zone if the operating time zones for the Server and Controller is different.



12.6.1 How to Set the Date & Time

1. Select the appropriate *Hour, Minute* and *Second* from the list box.
2. Do likewise for the *Day, Month*, and *Year* field.
3. Select the appropriate Time Zone from the *Choose Time Zone* drop-down list box.
4. Click on the button.

An additional function is implemented to allow user to maintain date and time synchronization with a timeserver. With synchronization on all of Access Easy Controller, user can ensure that events that happen in sequence on different controllers can be analysed correctly.


Time Synchronization Settings
Enable NTP Time Server for synchronization
Time Server IP address/DNS: 129.2.0.86
Disable synchronization if time difference between AEC and Time Server is > 15 minutes
Synchronize with Time Server Now
Last time synchronization status
Successfully synchronized on 7 Jul 03:00:13

1. Select *Enable NTP Time server for synchronization* and key in the IP address of the Timeserver PC.

NOTICE!
Refer to *Appendix E* on Setting up a Timeserver PC. *Time Server Address/DNS* input is the IP address of the PC being configured as a time server PC. Access Easy Controller is only able to synchronize with a NTP time server and will sync at 3 A.M daily automatically.
Auto Time synchronization at 3 A.M is only logged at transaction, however if user manually synchronise with the timer server, audit log will be logged.

2. Select *Disable synchronization if time difference between AEC and Time Server is >15 minutes* if you wants the Access Easy Controller to synchronize it's time even if the difference is more than 15minutes. This feature should be enabled to prevent the Access Easy Controller from synchrnoizing the wrong time with the Time server that is not accurate or timezone is incorrect.

Synchronizing date & time with a internet Time Server
Access Easy Controller is not able to synchronize with an internet Time Server if it is behind a firewall or proxy server. If it is outside the firewall or in a DMZ, you could enter the IP address of the Time Server in the Time Server *Address/DNS* input. Do not enter the domain name of the Time Server (eg. Time.windows.gov) in this input, Access Easy Controller will not be able to resolve the name to an IP address.

Synchronizing date & time with an intranet Time Server
It is recommended that the Access Easy Controller should synchronize it's date & time to an intranet (internal) Time Server. Most of the office has an internal Time Server, this Time Server will synchronize it's date & time with an internet (external) Time Server, while all other PCs in the office synchronize with this intranet Time Server.

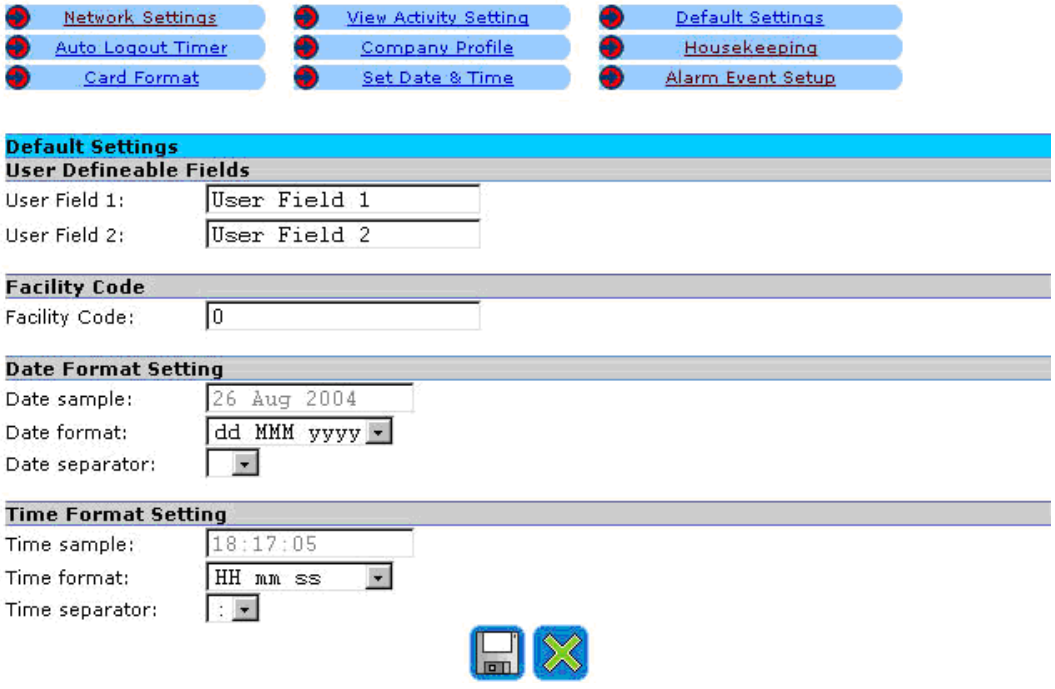
If the office does not have a intranet Time Server, you could setup any existing PC on the network as a Time Server, hence, the Access Easy Controller could synchronize its' date and time with this PC. There are numerous freeware available that you could install in this PC to synchronize its date and time with an external Time Server.

In *Appendix E,* we will briefly describe how you could setup a PC as a Time Server.

12.7 Default Settings

This setting allows user to define the descriptive name for the two user fields, *User Field 1* and *User Field 2*, and the Facility Code that will appear when Add Card or Batch Card is selected from *Card Assignment* menu. The user fields are limited to 20 character entries each while the Facility Code range depends on the Card Format in use. User can also select the Date Format and the Time Format that he prefers to view in the View Activity page and all the reports to be generated.

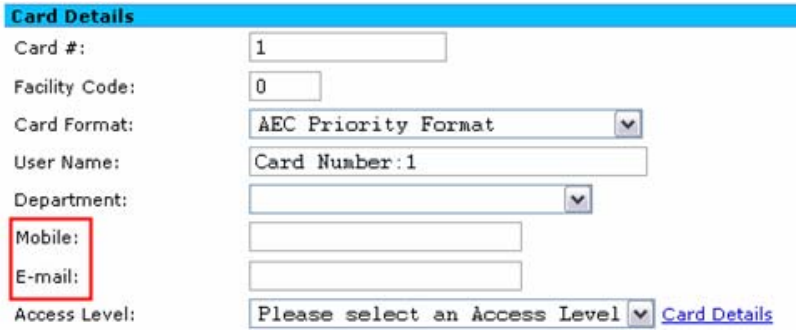
Click on *Default Settings* from the menu item list and you will see a screen as shown below.



12.7.1 How to Edit the User Definable Fields

1. Delete the default text and enter the new description for *User Field 1*.
2. Repeat for *User Field 2*.
3. The above example shows that Mobile is used in *User Field 1* and E-mail is used for *User Field 2*.
4. Click on the button.

After *User Field 1* and *User Field 2* are changed, user can then see Mobile and E-mail instead when user selects *Add Card* from *Card Assignment menu,* as shown below.



12.7.2 How to Edit the Facility Code

1.Delete the default text and enter the new *Facility Code* (you can obtain this code from your card supplier, enter "0" if the Card Format doesn't support Facility Code).

2.Click on the button.

User can then see the facility code appear as default when user selects *Add Card* or *Batch Card* from *Card Assignment* menu.

12.7.3 How to Edit the Date Format

1. Select the preferred *Date format* to be seen in the *View Activity* page and in all the reports generated.
2. Select a *Date separator* if desired.
3. Click on the button.

User can then see a sample of the date that will appear in the View Activity page and the reports to be generated in the *Date* sample box.

12.7.4 How to Edit the Time Format

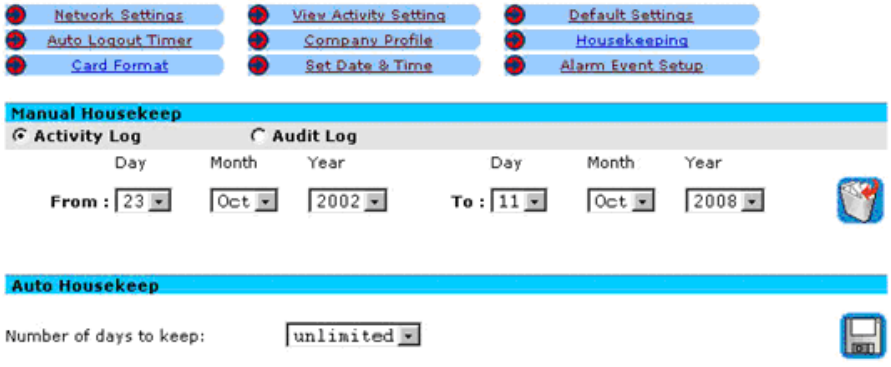
1. Select the preferred *Time format* to be seen in the *View Activity* page and in all the reports generated.
2. Select a *Time separator* if desired.
3. Click on the button.

User can then see a sample of the time that will appear in the View Activity page and the reports to be generated in the *Time sample* box.

12.8 Housekeeping

Housekeeping allows the user to manage the Activity Log and Audit Log in the system. User can delete the unwanted logs that are no longer required manually as well as to specify the number of days of the logs to be kept in the system and the system will store the logs of the most recent specified number of days only in the system.

Click on *Housekeeping* from the menu item list and you will see a screen as shown below.



12.8.1 How to Use the Manual Housekeep

1. Select either the Activity Log or the Audit Log to housekeep by selecting the respective radio button.
2. Select the Day, Month and Year of the From Date and the To Date. This range of dates are the dates in which the user would like to delete the Activity Log or the Audit Log (depending on which the user chooses) from the system.
3. After the range of date is selected, click on the button to clear the Log that falls within the date range.

12.8.2 How to Use the Auto Housekeep

1. Choose the number of days of both the Activity Log and Audit Log to be kept in the system. User are given a choice of 30, 60, 90 and 120 days. For example, if user chooses 30 days, the system will automatically delete the Activity and Audit Logs from the system if they are more than 30 days from today's date. User can also choose unlimited, which means the system will not delete the logs from the system.
2. Click on the button to save the settings.

12.9 Alarm Event Setup

An Alarm Event is any abnormal activity which we would like to monitor and be alert when such occurrence happens. All the alarm descriptions are listed below.

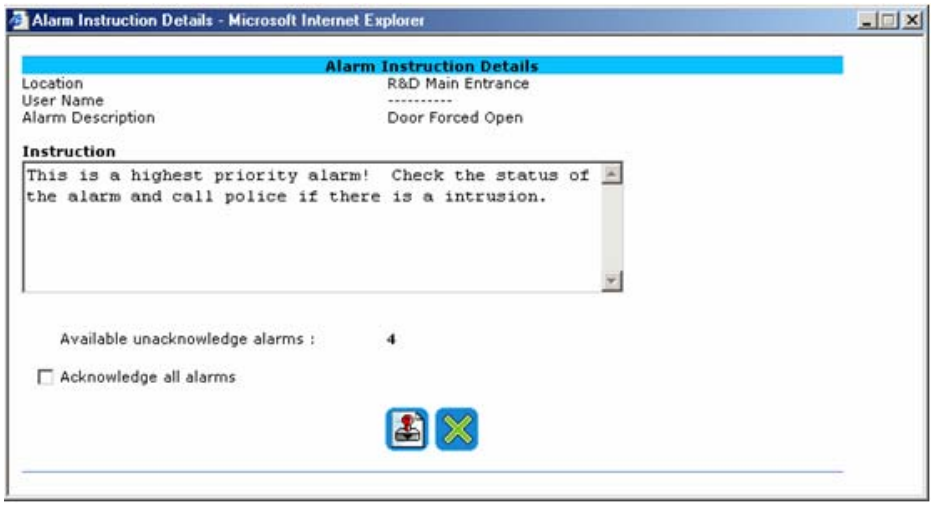
Access Denied	Input Point Fault - Opened
Access Denied - Card Disabled	Input Point Fault - Shorted
Access Denied - Passback	Invalid Card
Access Denied - Time APB	Invalid End Date
Access Denied - Wrong Pin	Invalid First Card Read
Alarm	Invalid Schedule
Convertor Communication Failed	Invalid Second Card Read
Dial In - Invalid Password	Invalid Start Date
Dial In - Invalid User Name	Panel AC Failure
Dial In - Lockout	Panel Disconnected
Disconnected from Server	Panel Not Registered
Door Contact - Input Fault - Opened	Panel Not Registered in Server
Door Contact - Input fault - Shorted	Panel Tamper
Door Forced Open	Reader Lockout
Door Held Open	Request To Exit -Input Fault - Opened
Duress	Request To Exit -Input Fault - Shorted
Exit Denied - Passback	System Halted
Guard Tour Key Not Remove	Time Synchronization Failed

The *Alarm Event Setup* provides the required settings which will affect how the *View Activities* will arrange the alarms and how it will respond to the user when acknowledged.

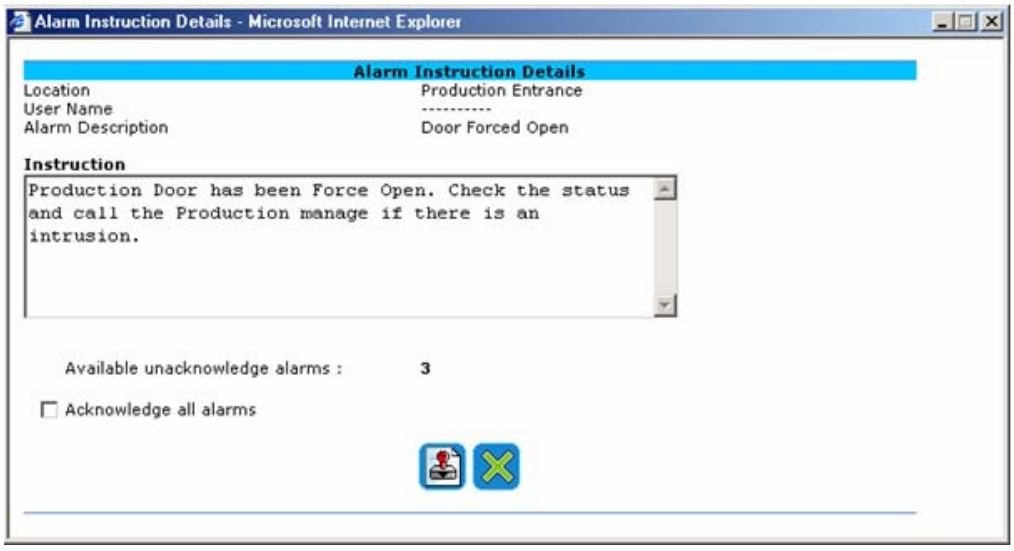
The setup includes :

1. Alarm Priority Setup
2. Alarm Event Condition Setup
3. Alarm Instruction Message Setup

Consider this as an example. You would like all the Door Forced Open alarm to be given the highest global priority. The earliest Door Forced Open alarm will have to be acknowledged first before the rest of the alarms with lower global priority. Furthermore, you would like to group the doors in terms of their location, such as R&D Dept, Production Dept, etc. These grouping will allow you to customize an *Alarm Instruction Message* for each group. Hence, when the operator acknowledges a Door Forced Open alarm of R&D Dept group from the *View Activity*, an instruction will be displayed on the screen as shown in the following screen shot


Alarm Instruction Details - Microsoft Internet Explorer
Alarm Instruction Details
Location
R&D Main Entrance
User Name
Alarm Description
Door Forced Open
Instruction
This is a highest priority alarm! Check the status of the alarm and call police if there is a intrusion.
Available unacknowledge alarms :
4
Acknowledge all alarms

While acknowledging a Door Forced Open alarm of Production Dept, a different instruction will be displayed on the screen as shown below.


Alarm Instruction Details - Microsoft Internet Explorer
Alarm Instruction Details
Location
Production Entrance
User Name
Alarm Description
Door Forced Open
Instruction
Production Door has been Force Open. Check the status and call the Production manage if there is an intrusion.
Available unacknowledge alarms :
3
Acknowledge all alarms

The system too provides a feature *Individual Alarm Priority*. This allows you to configure a very important location with a higher priority than other location when the same alarm is activated. For example, the Store Room is considered to be an important location to monitor. It is configured with an individual priority of 2, while the Door Forced Open alarm is configured with global priority 3. Hence, if the following Door Forced Open alarm is activated, the Store Room's Door Forced Open alarm will be listed on top of the rest even though it has occurred last.

Store Room Door Forced Open11:00am
R&D Room Door Forced Open10:00am
Production Room Door Forced Open10:30am
This Chapter will guide you step by step in configuring the Alarm Events to respond the way you prefer.

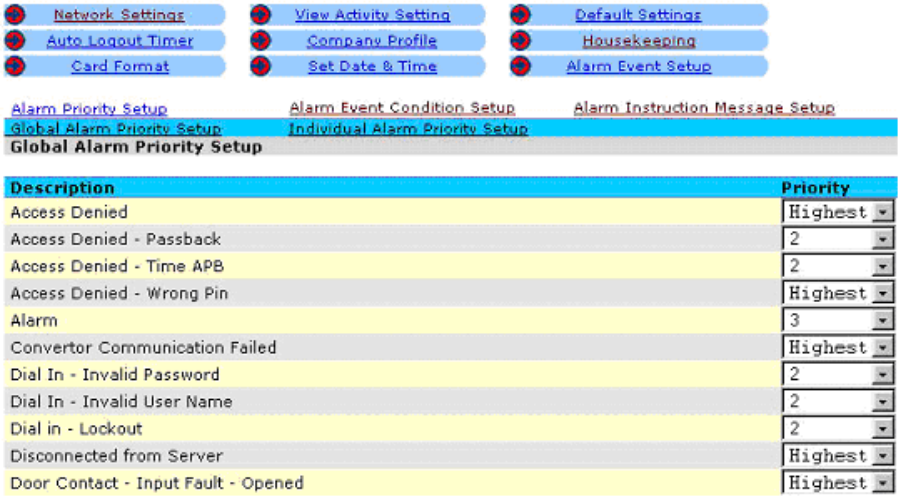
12.9.1 Alarm Priority Setup

Alarm Priority Setup can be grouped into *Global Alarm Priority Setup* and *Individual Alarm Priority Setup*. This section will describe how to configure Global and Individual Alarm Priority Setup.

How to Configure Global Alarm Priority Setup

This part of the setting allows you to define the hierarchy of priorities for alarms.

1. Click on *Alarm Event Setup* from the menu item list and you will see a screen as shown below. The default screen is the *Global Alarm Priority Setup* screen.



2. Select the priority of each type of alarm from the Priority list box. The priority of the alarms can range from 1 to 128, with priority 1 as the highest priority and is denoted by *Highest*, and priority 128 the lowest priority and is denoted by *Lowest*.

3. To complete the setting, click on the icon to save.

NOTICE!

View Activity will sort the alarms in the following order :

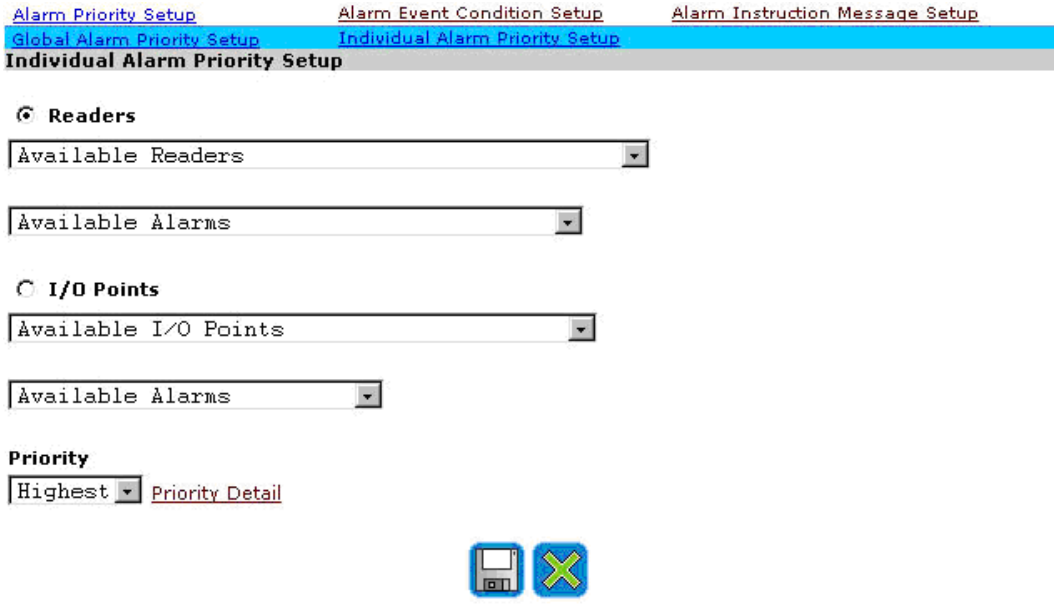
1. Priority
2. Date and Time of occurrence.

How to Configure Individual Alarm Priority Setup

This part of the setting allows you to define the hierarchy of priorities for individual location alarms.

1. From the *Global Alarm Priority Setup* screen, click on the Individual *Alarm Priority Setup* hyperlink. A screen as shown below appears.

2. Click on the button to add a new individual alarm priority to the system. The screen as shown below appears.



3. Select the appropriate option button.

If *Reader* is selected, you will need to select which Readers to assign this priority from the *Available Readers* list box. The *Available Alarms* allow you to choose which type of alarm this selected Reader will have the priority.

If *I/O Points* is selected, you will need only to select which Input Point to assign this priority.

4. Next select the level of priority from the *Priority list* box.

5. To save the setting, click on the button.

12.9.2 Alarm Event Condition Setup

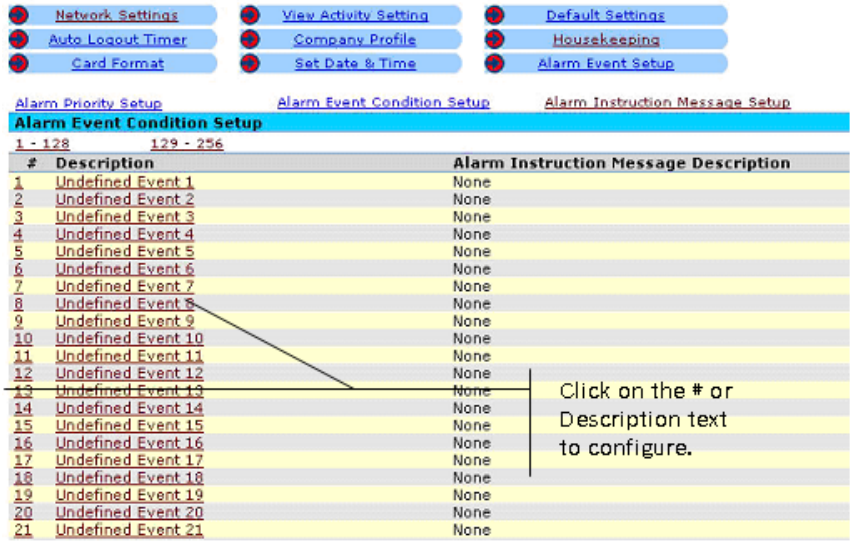
This part of the setting allows you to define up to 256 different Alarm Event. Each Alarm Event can consist of a combination of alarms, devices and Alarm Instruction Message.

An Alarm Event allows you to customize the Alarm Instruction Message that will be displayed when the user acknowledges an alarm from the *View Activity*.

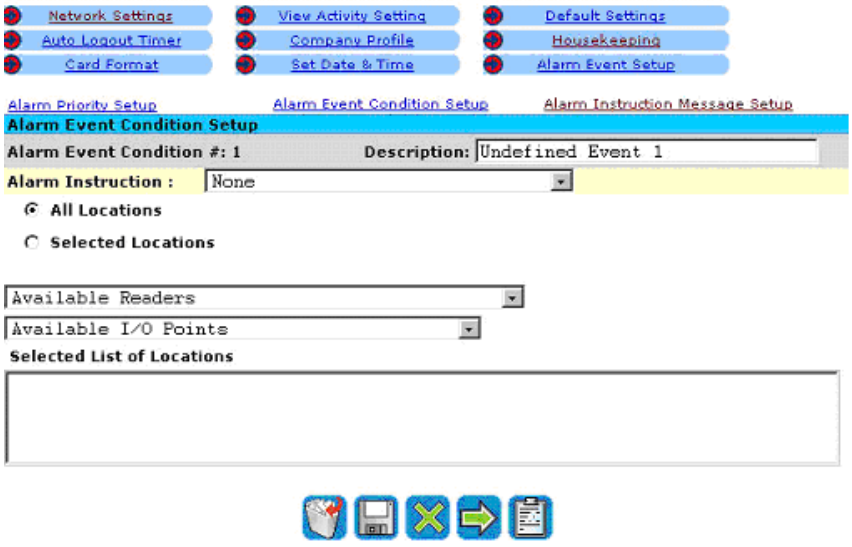
Referring back to the previous example, where you would like the user to see an instruction message for the Door Forced Open Alarm and Invalid Card Alarm in R&D Dept and a different instruction message for the Door Forced Open Alarm and Invalid Card Alarm in Production Dept.

You will need to configure 2 different Alarm Events. Let's use this example as we guide you through the configuration.

1. From the *Alarm Event Setup* screen, click on the *Alarm Event Condition Setup* hyperlink. The *Alarm Event Condition Setup* screen will appear as shown below.


Network Settings
View Activity Setting
Default Settings
Auto Logout Timer
Company Profile
Housekeeping
Card Format
Set Date & Time
Alarm Event Setup
Alarm Priority Setup
Alarm Event Condition Setup
Alarm Instruction Message Setup
Alarm Event Condition Setup
1 - 128
129 - 256
Description
Alarm Instruction Message Description
1 Undefined Event 1 None
2 Undefined Event 2 None
3 Undefined Event 3 None
4 Undefined Event 4 None
5 Undefined Event 5 None
6 Undefined Event 6 None
7 Undefined Event 7 None
8 Undefined Event 8 None
9 Undefined Event 9 None
10 Undefined Event 10 None
11 Undefined Event 11 None
12 Undefined Event 12 None
13 Undefined Event 13 None
14 Undefined Event 14 None
15 Undefined Event 15 None
16 Undefined Event 16 None
17 Undefined Event 17 None
18 Undefined Event 18 None
19 Undefined Event 19 None
20 Undefined Event 20 None
21 Undefined Event 21 None
Click on the # or Description text to configure.

2. Select any of the Undefined Events to configure an Alarm Event Condition. The following screen will appear.



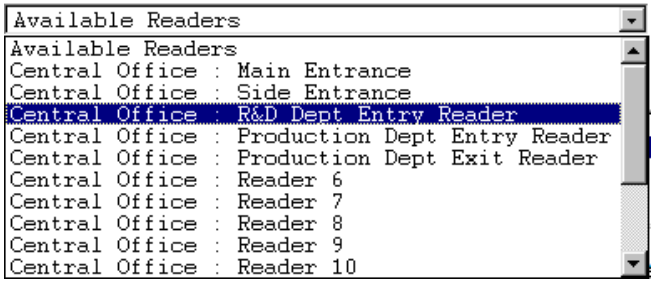
3. Enter a name for the Alarm Event in the *Description* textbox.
4. Choose the appropriate option button.

All Locations	All Readers, Input Points and Output Points are monitored for the events.
Selected Locations	Only the Devices in the Selected List of Locations are monitored for the events.

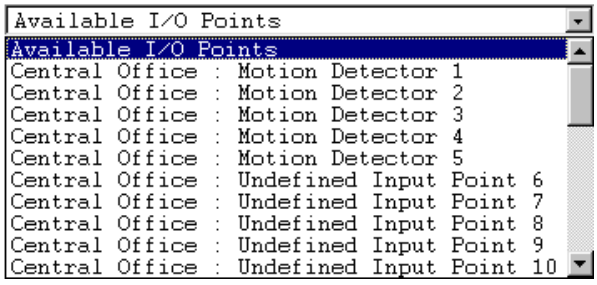
In the case of this example, choose *Selected Locations*, as we only want those doors belonging to R&D dept to display the alarm instruction message.

5. If *Selected Locations* is chosen, you will need to select the Readers or Input Points or Output Points from the pull-down list box.

The *Available Readers* list box contains all the readers that are available in the entire system.

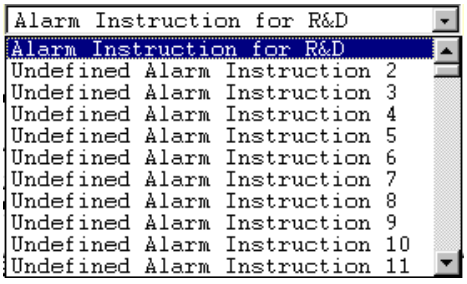

Available Readers
Available Readers
Central Office : Main Entrance
Central Office : Side Entrance
Central Office : R&D Dept Entry Reader
Central Office : Production Dept Entry Reader
Central Office : Production Dept Exit Reader
Central Office : Reader 6
Central Office : Reader 7
Central Office : Reader 8
Central Office : Reader 9
Central Office : Reader 10

The *Available I/O Points* list box contains all the Input Points and Output Points that are available in the entire system.


Available I/O Points
Available I/O Points
Central Office : Motion Detector 1
Central Office : Motion Detector 2
Central Office : Motion Detector 3
Central Office : Motion Detector 4
Central Office : Motion Detector 5
Central Office : Undefined Input Point 6
Central Office : Undefined Input Point 7
Central Office : Undefined Input Point 8
Central Office : Undefined Input Point 9
Central Office : Undefined Input Point 10

Choose the desired Readers, Input Points or Output Points to be added to the *Selected List of Locations* by clicking on the description of the device. For this example, R&D Dept Entry Reader is selected, as shown above.

6. After selecting all the devices to be included in the *Selected List of Location,* the next step is to select the relevant *Alarm Instruction Message* that you would like the user to see when they acknowledge the alarm.
7. The *Alarm Instruction* list box provides a list of available messages that you could select.

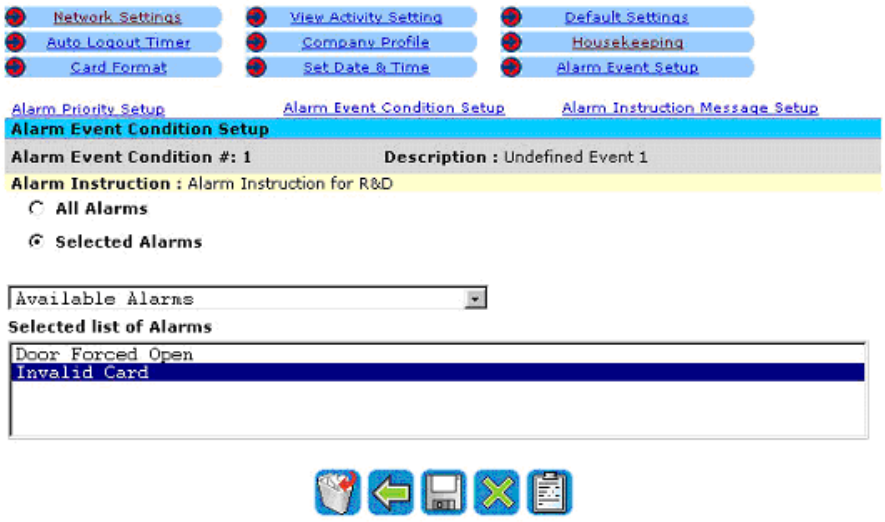

Alarm Instruction for R&D
Alarm Instruction for R&D
Undefined Alarm Instruction 2
Undefined Alarm Instruction 3
Undefined Alarm Instruction 4
Undefined Alarm Instruction 5
Undefined Alarm Instruction 6
Undefined Alarm Instruction 7
Undefined Alarm Instruction 8
Undefined Alarm Instruction 9
Undefined Alarm Instruction 10
Undefined Alarm Instruction 11

Select the appropriate Alarm Instruction Message as shown above.

NOTICE!
Alarm Instruction Messages are configured in the Alarm Instruction Message Setup. Please refer to the next section Alarm Instruction Message Setup for details.

8. Click the to save and go to next page.

9. The next page that appears allows you to select the type of events that will display the Alarm Instruction Messages that you have just selected.

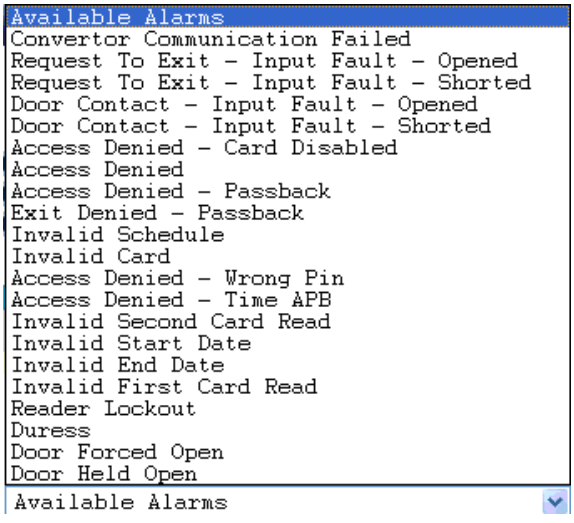


10. Choose the appropriate option button.

All Alarms	All the alarms will use the same Alarm Instruction Message as configured earlier.
Selected Alarms	Only the Alarms in the Selected List of Alarms will display the Alarm Instruction Message as configured earlier.

In this example, choose *Selected Alarms*, as we only want those Door Forced Open Alarm and Invalid Card Alarm to display the alarm instruction message.

11. If *Selected Alarms* is chosen, you will need to select the type of alarms from the pull-down list box. The Available Alarms list box contains all the different types of alarms that are available in the entire system.



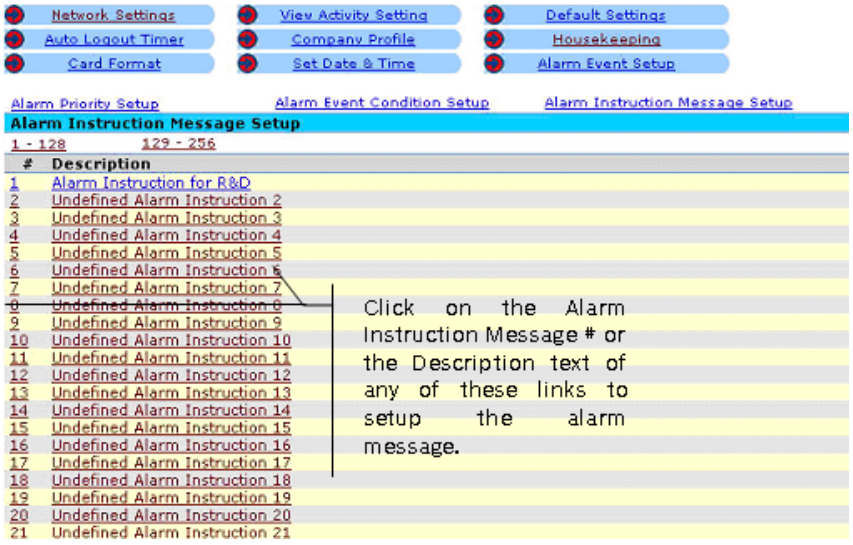
Choose the desired alarms to be added to the *Selected list of Alarms* by clicking on the description of the alarm. For the example, *Door Forced Open* and *Invalid Card* are selected.

12. Lastly, click on to save the settings.

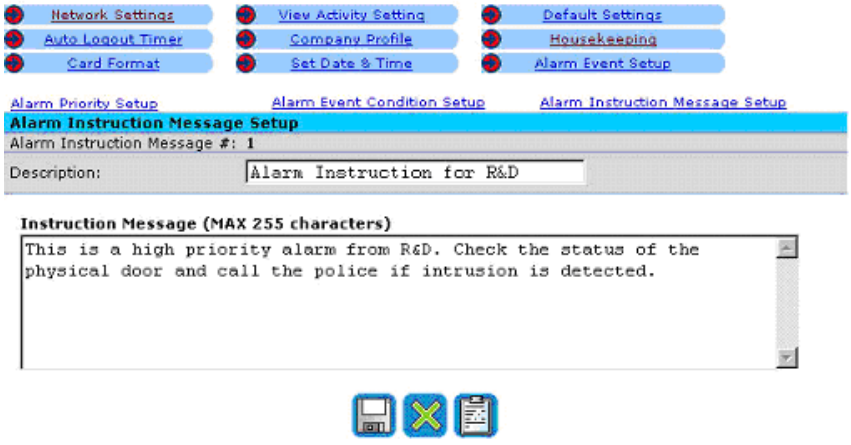
12.9.3 Alarm Instruction Message setup

This part of the setting allows you to define up to 255 different *Alarm Instruction Message* for the *Alarm Event Conditions*.

1. From the *Alarm Event Setup* screen, click on the *Alarm Instruction Message Setup* hyperlink. The *Alarm Instruction Message Setup* screen will appear as shown below.


Network Settings
View Activity Setting
Default Settings
Auto Logout Timer
Company Profile
Housekeeping
Card Format
Set Date & Time
Alarm Event Setup
Alarm Priority Setup
Alarm Event Condition Setup
Alarm Instruction Message Setup
Alarm Instruction Message Setup
1 - 128
129 - 256
Description
1 Alarm Instruction for R&D
2 Undefined Alarm Instruction 2
3 Undefined Alarm Instruction 3
4 Undefined Alarm Instruction 4
5 Undefined Alarm Instruction 5
6 Undefined Alarm Instruction 6
7 Undefined Alarm Instruction 7
8 Undefined Alarm Instruction 8
9 Undefined Alarm Instruction 9
10 Undefined Alarm Instruction 10
11 Undefined Alarm Instruction 11
12 Undefined Alarm Instruction 12
13 Undefined Alarm Instruction 13
14 Undefined Alarm Instruction 14
15 Undefined Alarm Instruction 15
16 Undefined Alarm Instruction 16
17 Undefined Alarm Instruction 17
18 Undefined Alarm Instruction 18
19 Undefined Alarm Instruction 19
20 Undefined Alarm Instruction 20
21 Undefined Alarm Instruction 21
Click on the Alarm Instruction Message # or the Description text of any of these links to setup the alarm message.

2. Click on any of the Undefined Alarm Instruction to configure an Alarm Instruction Message. The following screen will appear.


Network Settings
View Activity Setting
Default Settings
Auto Logout Timer
Company Profile
Housekeeping
Card Format
Set Date & Time
Alarm Event Setup
Alarm Priority Setup
Alarm Event Condition Setup
Alarm Instruction Message Setup
Alarm Instruction Message Setup
Alarm Instruction Message #: 1
Description:
Alarm Instruction for R&D
Instruction Message (MAX 255 characters)
This is a high priority alarm from R&D. Check the status of the physical door and call the police if intrusion is detected.

3. Enter a name for the Alarm Instruction Message in the *Description* textbox.
4. The Instruction Message textbox provides a space for you to enter up to 255 characters. You could enter the instruction that you want to pop up to the screen when the user acknowledges the alarm. Please refer to the previous section *How to Setup Alarm Event Condition* for the assignment of Alarm Instruction Message to Alarm Event Condition.
5. To complete the setup click on to save the settings.

13 Report Generation

Report Generation feature allows us to generate report for activities which have occurred. It has a filtering mechanism to find and sort out activities based on the criteria set by the user. The criteria that could be defined are:

1. Date/Time
2. Devices
3. Card Holders
4. Events

By combining the correct combination, the user could generate a detail and specific report. The criteria can also be saved for further use.

NOTICE!

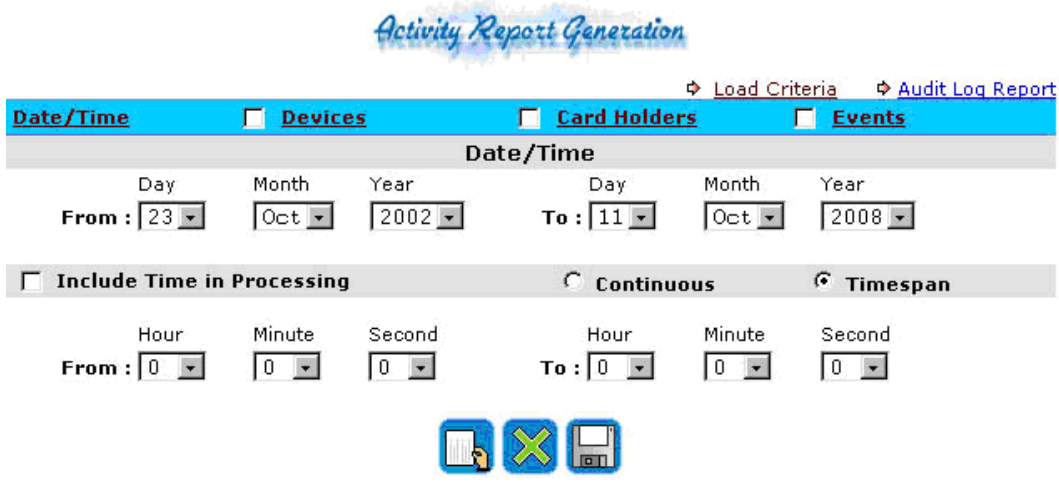
1. The more criteria is defined, the more accurate and precise is the report. However, an incorrect mix of criteria will result in not finding the information you need. Please refer to *Appendix A Selecting Events, Devices And Cardholders For Report Generation* for information on selecting the criteria.

2. The Report Generation can only generate 2000 records each time. Users will be warned by a message box to reduce the range of the Date and Time selection if the records exceed 2000.

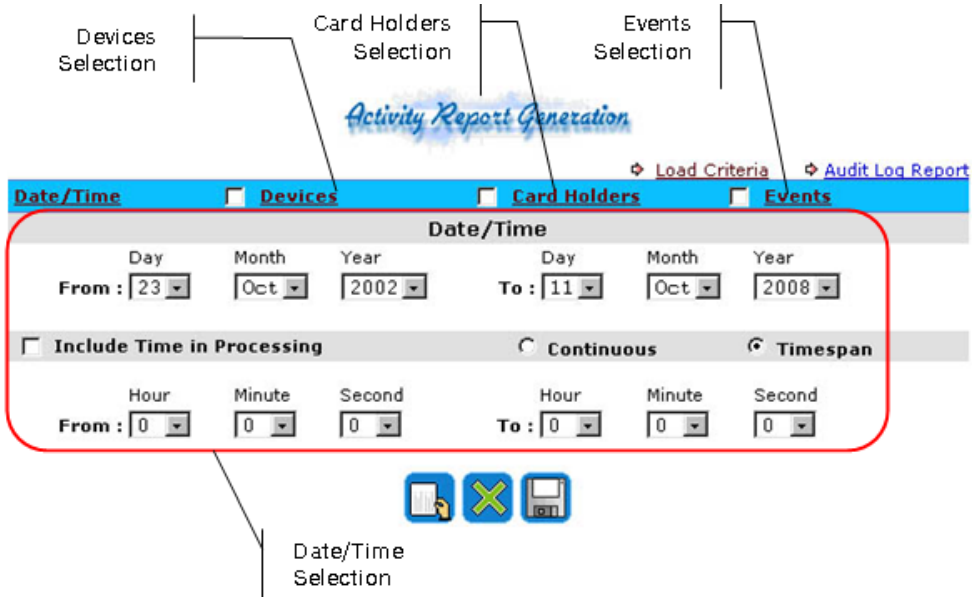
The following sections will provide a step-by-step guide to configuring a criteria for report generation purpose.

13.1 How to Set Criteria for Report Generation

1. Select the *Report Generation* hyperlink on the Left Pane and the *Report Generation* page will appear as shown below.



Now let us take a brief look at the screen layout of the *Report Generation* page.



In order to successfully generate a report, you will need to specify the criteria for the Access Easy Master. The following is a table which will explain the purpose and usage of each Selection.

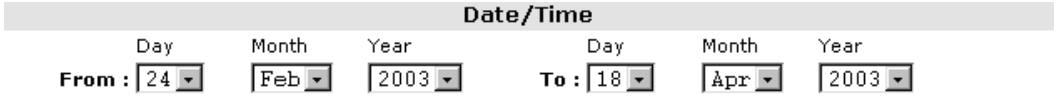
Date/Time Selection	Date is a compulsory selection. User needs to identify what is the range of date the report should cover. The activities that occur within these dates will be listed in the report. Time, however, is an optional selection. User could specify the time period of interest that the activities have occurred. The activities that occur during this period of time will be listed in the report.
Devices Selection	This is an optional selection. It lists devices such as Reader and I/O Point to choose. The activities that are generated by the selected list of Devices will be listed in the report.
Card Holders Selection	This is an optional selection. Specific Card Holder can be chosen. The activities that are generated by the selected list of Card Holders will be listed in the report.
Events Selection	This is an optional selection. User could specify the type of activities to be included in the report.

By creating a combination of all the selections, the user would print a summary of the required report in the shortest time.

Let us look into an example as we go through the steps of configuring the criteria:

We would like to print out all the Door Forced Open Alarm (Event) that occur to R&D Main Entrance Door (Device) from 24 Feb 2003 to 18 April 2003 (Date) between 8am to 5pm (Time).

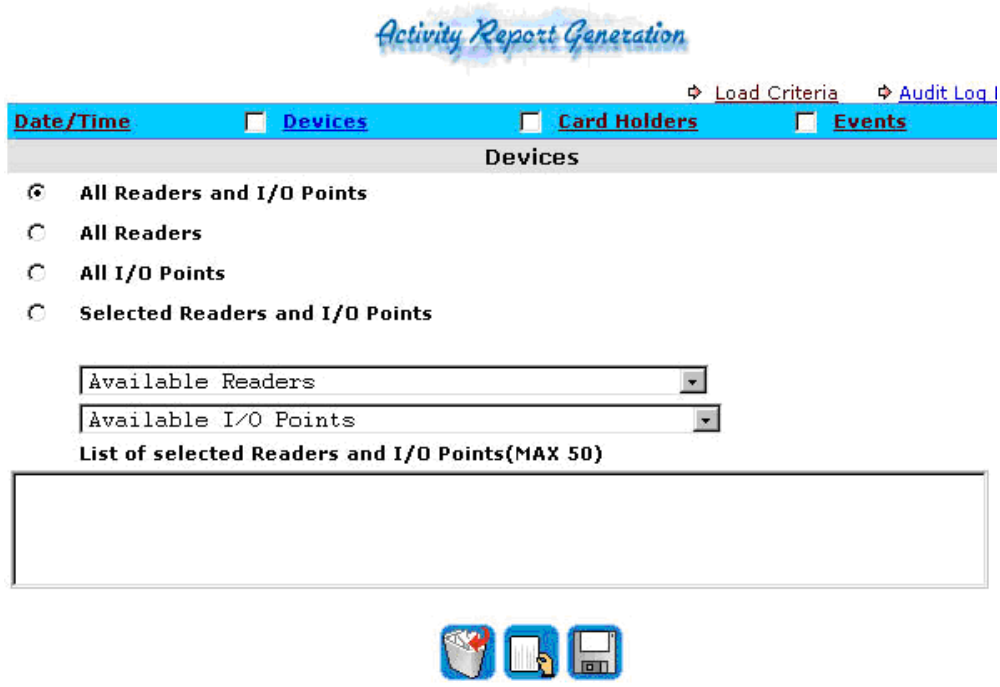
2. First of all, select the From date and the To date from the Date/Time entry.



3. Next, select the *From* time and the *To* time and check the check box for Include Time in Processing. User also has to select whether the time is Continuous or according to Timespan by selecting the appropriate radio button. Continuous means that the report generated would be all the way from the starting time of the starting date to the end time of the ending date. Timespan means that the report will be generated from the starting time to the ending time for each day in the selected date range.

NOTICE!
If the check box for Include Time in Processing is not selected, the report will be generated according to the other selected criteria, without any time filtering.

4. To configure the Devices selection, click on the *Devices* hyperlink and the following screen will appear.



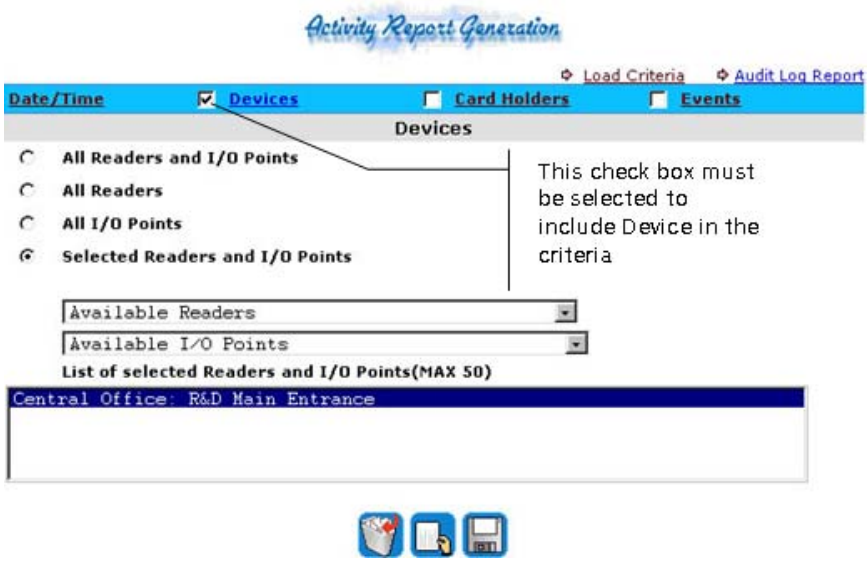
5. Choose the appropriate option button.

All Readers and I/O Points	All activities of devices such as Readers, Input Points and Output Points will be taken into account in the generation of report.
All Readers	Only activities of Readers will be taken into account in the generation of report. Selection of this option will result in only Readers' activities to be included in the report.
All I/O Points	Only activities of Input Points and Output Points will be taken into account in the generation of report. Selecting this option will result in only I/O Points' activities to be included in the report.
Selected Readers and I/O Points	Only selected devices' activities listed in the List of selected Readers and I/O Points will be taken into account in the generation of report.

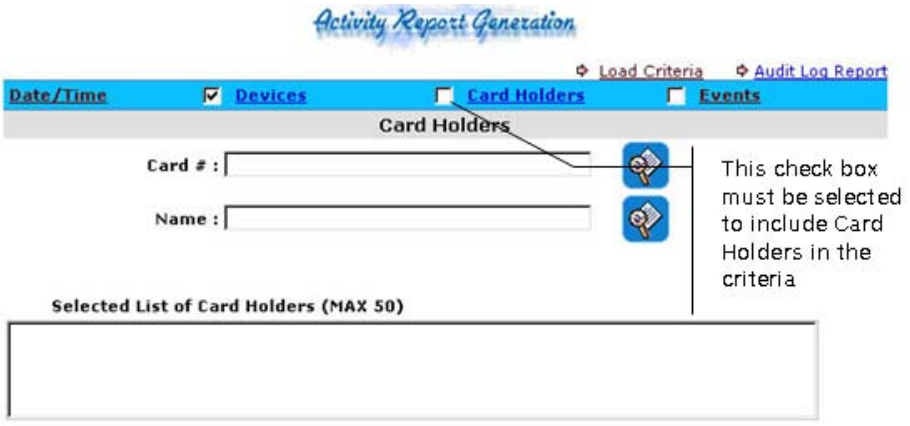
In this example, choose *Selected Readers and I/O Points*, as we only want Door Force Open Alarms from R&D Main Entrance to be included in the report, as shown below.

6. Check the *Devices* check box to indicate that Devices selection is to be included in the criteria, as shown below.

NOTICE!
The selected Device will not be taken into consideration during the generation of the report if the check box for Devices is not selected.



7. Click on the *Card Holders* hyperlink to go to the next configuration page. A screen as shown below appears.



8. This page allows you to configure the Cardholders that should be included in the report criteria. Check the *Card Holders* check box to include this selection in the criteria. Take note that some of the activities do not have the cardholder's ID included. Activities such as Panel Tampered, Exit Grant, Door Force Open, etc, do not require the Card Holder selection to be configured.

NOTICE!
Care should be taken when including the Card Holders selection into the criteria. By including the Card Holders into the criteria, activities that do not require this will not appear in the report, such as Panel Tampered, Exit Grant, Door Force Open, etc. Please refer to A*ppendix A Selecting Events, Devices And Cardholders For Report Generation* for a guide in selecting the correct combination of selection for criteria.

In the case of this example, we will not select the Card Holder selection as the activities we need to generate do not require this selection, which is Door Forced Open Alarm from R&D Main Entrance door.

NOTICE!
The Card Holder will not be taken into consideration during the generation of the report if the check box for Card Holders is not selected.

9. For the activities that require the Card Holders selection to be included in the criteria, follow step 10 to 14.
10. Only cardholders' ID indicated in the *Selected List of Card Holders* will be included in the criteria. To add a cardholder's ID to the list, you could search by *Card #* or by Name.
11. To search by Card ID, enter the Card ID in the *Card #* text box and click on the corresponding button. Access Easy Master will search through the card database and list out the cards that have the ID as shown on the following page.

12. Click on the name of the cardholder to add to the *Selected List of Card Holders*.

NOTICE!
If there are 2 or more IDs that are the same but with different facility code or card format, the search will still show all of them in the *List of Persons Found*.

13. To search by cardholder's name, enter the name in the Name textbox and click on the corresponding button. Access Easy Master will search through the card database and list out the cards that has similar name as shown below.

NOTICE!

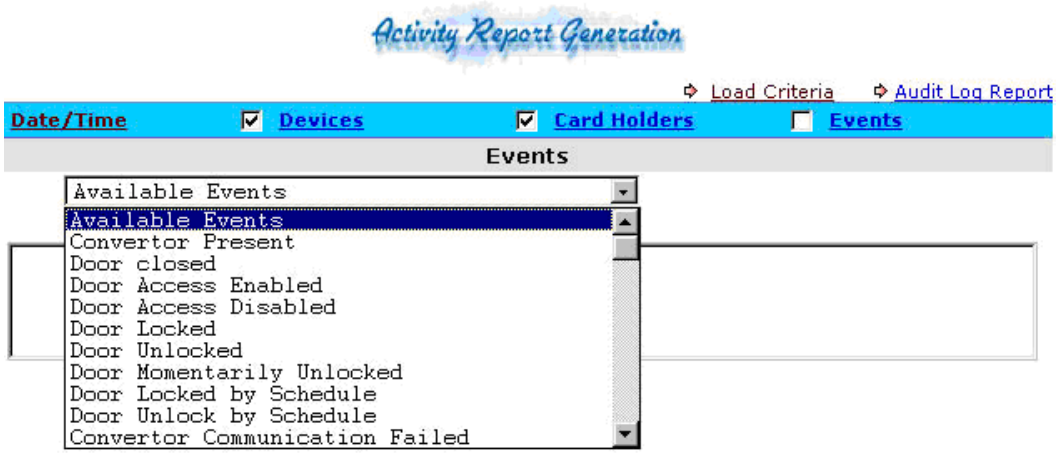
The above screen shows 2 names in the *List of Persons Found*. This is the result of searching the name "John". Access Easy Master will show all names that are similar, allowing the user to find the one that he needs without knowing the full name of the cardholder.

14. Click on the name of the cardholder to add to the *Selected List of Card Holders*.
15. The next step will be to configure the Events selection. Click on the *Events* hyperlink and the following screen will appear.

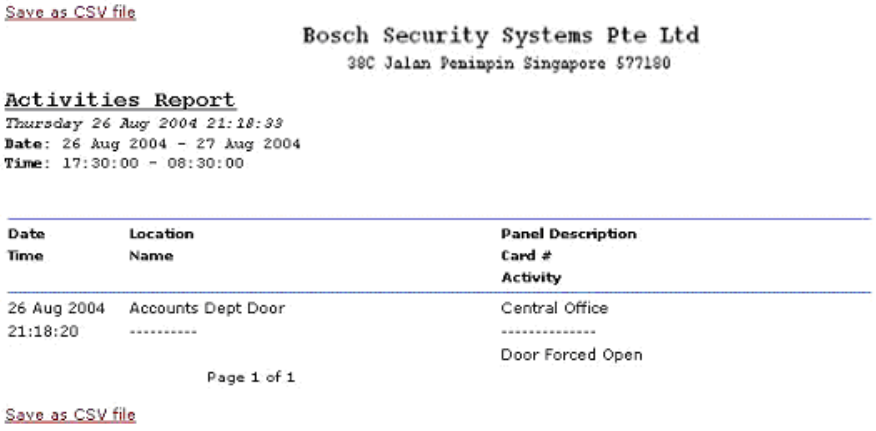
NOTICE!

The Events will not be taken into consideration during the generation of the report if the check box for Events is not selected.

16. Select the relevant events from the pull-down list. Click on the events, such as Door Forced Open, to add them to the *Selected List of Events*.



17. To start generating the report, click . The following is a sample of the report generated.



NOTICE!
The report can be saved in a CSV format. This format is basically a text file in which the data are separated by a comma(,). To save in CSV format, click on the *Save as CSV file* and a dialogue box will appear for you to download the file to your local PC.

13.2 How to Save Criteria for Future Use

Criteria created in the previous section can be saved in the Access Easy Master for future use. This is very helpful when the user needs to generate daily, weekly or monthly reports. By saving the criteria, the user need not re-configure the selections. Instead he could just call out the criteria that has been saved previously and generate the report with new Date and Time settings.

The following step shows you how to save the criteria in the Access Easy Master.

1. After configuration the criteria, click on the to save the criteria. The following screen shows the *Save Criteria* page.

2. Type a name in the *Save As* textbox and click on the button.

13.3 How to Generate Report Using Saved Criteria

To generate reports using previously saved criteria, you will need to load the criteria from the Access Easy Master.

1. From the *Report Generation* page, click on Load Criteria at the top right corner of the page and the *Activity Report Generation* screen will appear as shown below.

2. You could now select the criteria from the *List of Criterias*.

3. After selecting the criteria that you need, click on the to load it.
4. The screen will refresh and the *Report Generation* page will be shown with the settings of the loaded criteria. Now all you need to do is set the Date and Time range and you could click to generate your report based on the loaded criteria.

13.4 How To Generate Audit Log Report

Audit Log records all the changes to the system parameters and who made the changes. It is a means to trace back what was done to the system by the login user. There are 2 types of audit trail report that can be generated, they are:

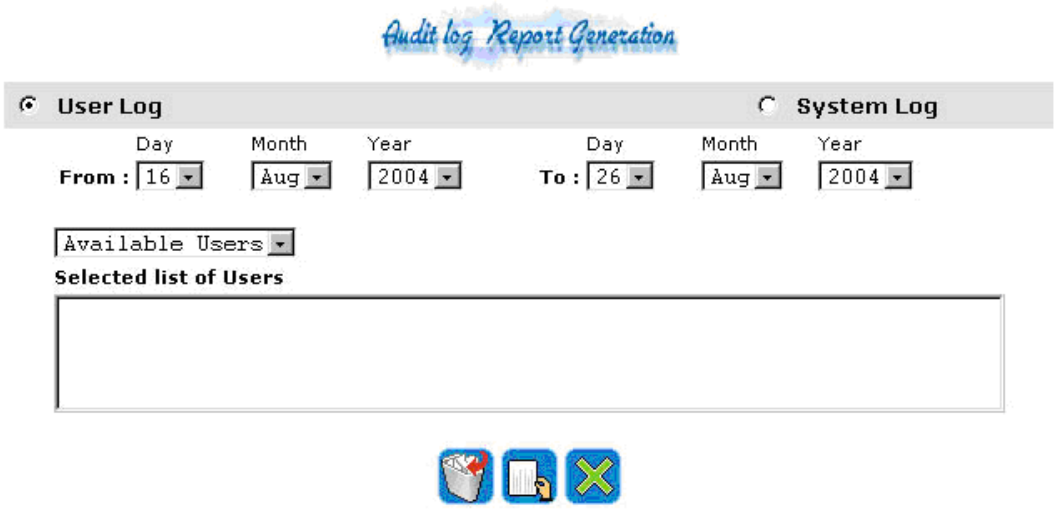
- User Log
- System Log

The following section provides a step-by-step guide to generate the reports.

13.4.1 User Log

The User Log provides a report on who has login and when it was done. It also captures the changes done by the User in the system.

1. From the *Report Generation* page, click on Audit Log Report and the *Audit Log Report* page will appear as shown below. By default, the *User Log* page is shown.



2. Select the *From* Date and the *To* Date.
3. The *User Log Report* allows you to select to generate report for all Users or selected Users only. To generate a report for all Users, just click on the , leaving the *Selected list of Users* blank. To generate a report for selected User, select the users from the pull-down list by clicking on the name of the user.
4. Click on to start generating the Log. The following shows a sample of the report generated for Vincent.

Bosch Security Systems Pte Ltd
38C Jalan Peminpin Singapore 577180

User Log
Saturday, 13 Sep 2003 11:22:32

From : 03 Sep 2003
To : 13 Sep 2003

Date/Time	Name	Action
06 Sep 2003 11:26:36	Vincent	Logged in
06 Sep 2003 11:32:48	Vincent	Logged out
11 Sep 2003 16:20:47	Vincent	Logged in
11 Sep 2003 17:28:05	Vincent	Logged in
11 Sep 2003 17:37:20	Vincent	Logged out
12 Sep 2003 23:55:12	Vincent	Logged in
12 Sep 2003 23:57:44	Vincent	Logged in
13 Sep 2003 00:03:33	Vincent	Logged out

13.4.2 System Log

The System Log provides a report on the system status.

1. To generate the System Log, select the radio button for *System Log*.
2. Click on to start generating the Log.

The following is a sample of the report.

Bosch Security Systems Pte Ltd
38C Jalan Peminpin Singapore 577180

System Log
Friday, 23 Dec 2005 14:05:42

Product Name	:	AEMC 2.1.29f-2
Hardware Address(MAC)	:	00:04:5F:81:2D:1D
Internet Address	:	172.16.10.99
Serial number	:	7D531C1BE471
Panel count	:	3
User count	:	1

Go to Wsync Log

```
runlevel (to lvl 3)   2.4.20-31.9      Mon Dec 12 11:20 - 14:05 (11+02:45)
reboot   system boot  2.4.20-31.9      Mon Dec 12 11:20         (11+02:45)
shutdown system down  2.4.20-31.9      Mon Dec 12 11:19 - 14:05 (11+02:46)
runlevel (to lvl 6)   2.4.20-31.9      Mon Dec 12 11:19 - 11:19  (00:00)
```

The report provides some critical information such as :

Hardware Address (MAC)	This is the physical address of the Access Easy Master. It is a unique number. We could use this number to set the IP address of the Access Easy Master using the ARP command. Please refer to the Chapter How to Configure the IP address.
Internet Address	This is the IP address of the Access Easy Master.
Serial Number	Each SAM in the Access Easy Master has a unique number. It serves as a license to the owner. If the owner wants to increase the number of login User or connect more Access Easy Controller to the Access Easy Master, he will have to register with Bosch using this number.
Panel Count	The total number of Access Easy Controller s that are licensed and connected to the Access Easy Master.
User Count	The total number of Login Users that are licensed.
Go to Wsync log	Shows the wsync log between server and panel.

14 Database Backup

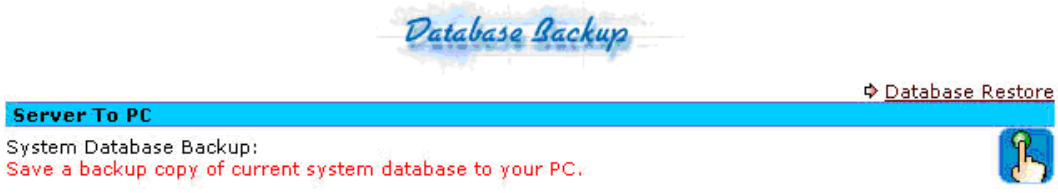
The *Database Backup* allows the user to save a backup copy of current system database to the local PC. It provides downloading of information which relates to the setting up of Access Easy Master, e.g Schedules details, Card Readers parameters, etc. It allows user to download the history of the Activity and Attendance in Comma Separated Variable (CSV) format.

The *Database Backup* also allows user to restore the database back to the Access Easy Master. It acts as a restore utility.

The following sections will guide you to perform both the operations.

14.1 How to Perform Database Backup

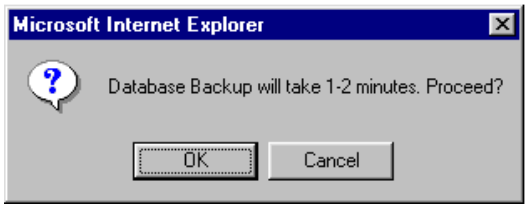
To activate Database Backup, click on *Database Backup* from the Left Pane. A screen as shown below appears.


Database Backup
Database Restore
Server To PC
System Database Backup:
Save a backup copy of current system database to your PC.

1. To start the backup, click on .

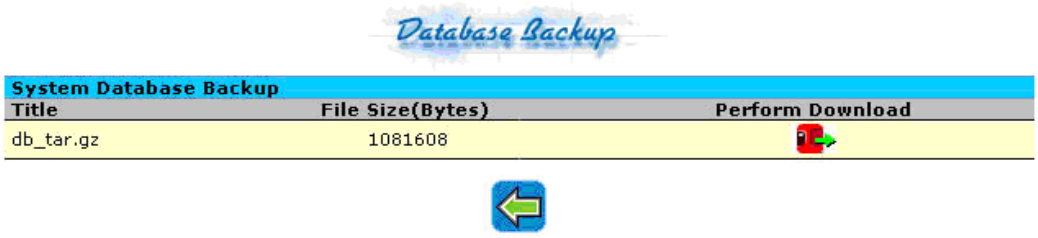
NOTICE!
A Database Backup typically takes about 1-2 minutes. During this period, it is advisable not to change other system parameters. However, the Access Easy Master and the Access Easy Controllers will not be affected by the action. All operations, such as door access and alarm monitoring, will still operate as usual.

2. A dialogue box will appear, confirming whether to proceed with the backup. Database backup will take 1 ~ 2 minutes.

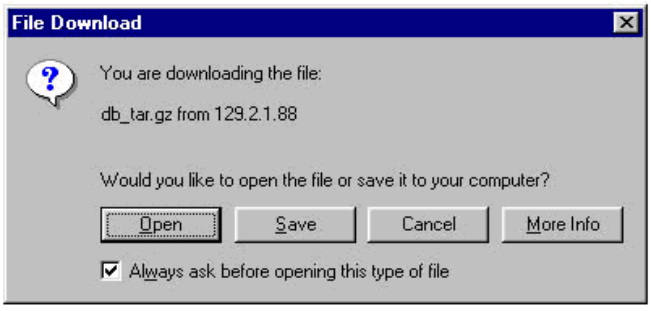


3. Click on [OK] to proceed with the database backup operation.
4. During backup, the message *Database backup in progress...* will appear on the screen.

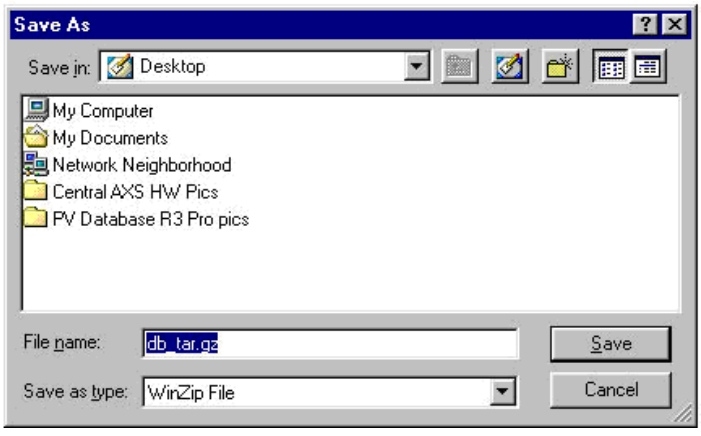
5. Once the backup is complete, a new screen will appear as shown below.



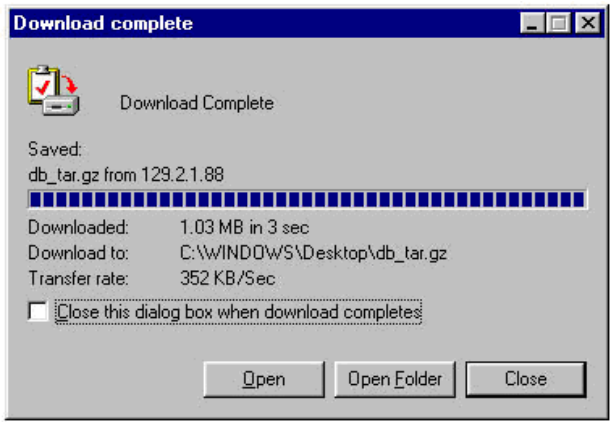
6. You could now save the db_tar.gz file to your local PC by clicking on the button.
7. The File Download box will appear, showing the file to be downloaded and the IP address of the Access Easy Master.


File Download
You are downloading the file:
db_tar.gz from 129.2.1.88
Would you like to open the file or save it to your computer?
Open
Save
Cancel
More Info
Always ask before opening this type of file

8. Click on [Save] to save the file to your local PC.
9. The user will be prompted to choose a location and file name to save the file.

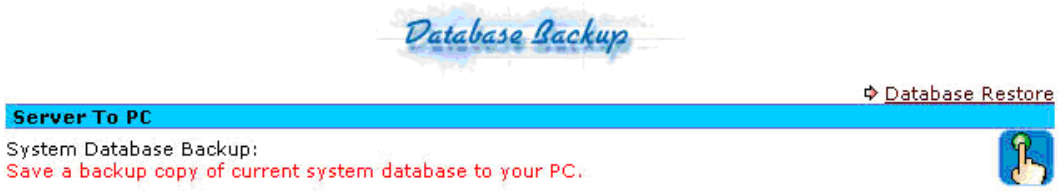


10. When the download is completed, the *Download Complete* box will appear.



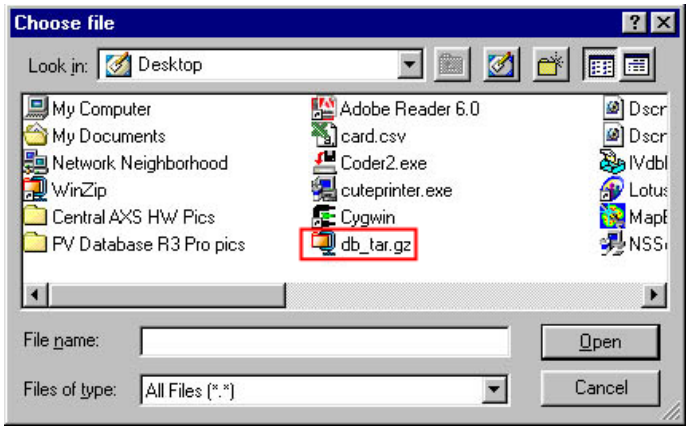
14.2 How To Restore System Database

To activate Database Backup, click on *Database Backup* from the Left Pane. A screen as shown below appears.


Database Backup
Database Restore
Server To PC
System Database Backup:
Save a backup copy of current system database to your PC.

1. Click on the Database Restore link at the top right corner of the page and the *Database Restore* page will appear as shown below.

2. Click on the *Browse* button to bring up the *Choose File* dialogue box as shown below.



3. Chose the db_tar.gz file and click the [Open] button.

4. To start the restore process, click on the button.

After successfully restoring the system database to the Access Easy Master, you will need to re-boot the Access Easy Master for the database to take effect.

NOTICE!

A Database Restore typically takes about 1-2 minutes. During this period, it is advisable not to change other system parameters. However, the Access Easy Master and the Access Easy Controller s will not be affected by the action. All operations, such as door access and alarm monitoring, will still operate as usual.

It is recommended that you perform a syncronisation of the Access Easy Master database to Access Easy Controller after you restore the database. Please refer to Chapter 9, How to add Access Easy Controller on the syncronsation operation.

15 Reboot, Shutdown and Logout

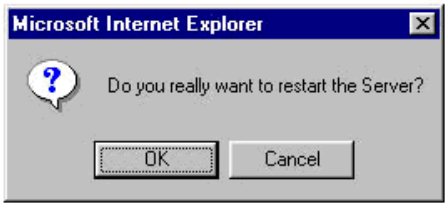
15.1 Reboot Function

The Reboot function allows user to reboot the server after upgrading to the system software is completed or in order to allow changes made to take effect, especially changes made to Network Setting, Panel's IP Address.

CAUTION!
During a Reboot, it is important that the Database Backup function is carried out before proceeding to reboot the Access Easy Master.

Reboot can be activated only from the Left Pane menu item.

1. From any menu item page, click on the Reboot link from the Left Pane. The following dialog box appears for confirmation.



2. Click on the OK button to proceed.
3. It takes a few minutes for the process to complete (see NOTICE).

NOTICE!
During the rebooting process, the Access Easy Master disconnects itself from the computer and the web page on the computer screen will show "Rebooting System..." before the web page becomes blank. User must close and re-launch the web browser program. Login to Access Easy Master again after the process is completed.

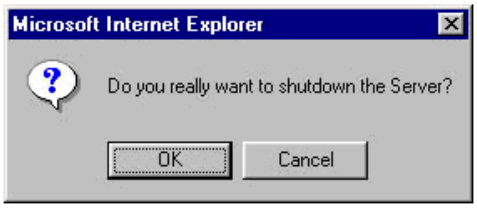
Once the Server is up and running again, please re-enter the Server URL Address and proceed with the Login.

15.2 Shutdown Function

The Shutdown function allows user to stop the Access Easy Master system properly if the user is required to.

Shutdown can be activated only from the Left Pane menu item.

1. From any menu item page, click on the *Shutdown* link from the Left Pane. The following dialog box appears for confirmation.



2. Click on the OK button to proceed.
3. It takes about 2 minutes for the system to shutdown.

CAUTION!
During the shutting down process, the Access Easy Master disconnects itself from the computer and the web page on the computer screen will show "System shutting down...".

15.3 Logout Function

The Logout function allows the user to do a proper exit from the web browser.

Logout can be activated only from the Left Pane menu item.

From any menu item page, click on the *Logout* link from the Left Pane. The web browser will logout immediately without any prompt. To login again, refer to *Chapter 3 Logging In and Understanding Access Easy Master Main Menu, Logging Into Access Easy Master*.

16 Panels Admin

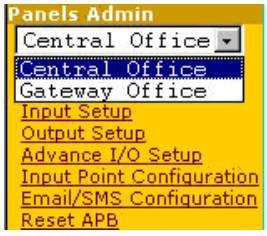
Panels Admin refers to the administration and configuration of individual Access Easy Controller, which are currently connected to the Access Easy Master.

Under *Panels Admin* menu of the Access Easy Master main menu, you will see the various parameters to configure for each individual Access Easy Controller such as *Access Groups, Card Readers, Input Setup, Output Setup Advance I/O Setup, Input Point Configuration, Email/SMS Configuration* and *Reset Anti-Passback* settings.

Panels Admin provides the Server Administrator the convenience of centrally accessing and configuring individual Access Easy Controllers that are currently having a connection with it.

16.1 How To Choose Individual Panel To Admin

The Access Easy Master is able to detect which Access Easy Controller are setup and Panels that are currently having a connection to it. For Panels that are off-line due to network problem, they will still be shown in the list of Panels in Panels Admin. Their settings can still be changed and when the Panels are connected, the new settings will be synchronized to the Panels. As shown below, 2 Panels named Central Office and Gateway Office are currently setup to the Access Easy Master.



To configure any item (*Access Groups, Card Readers, Input Setup, Output Setup, Advance I/O Setup, Input Point Configuration, Email/SMS Configuration or Reset APB*) of a particular Access Easy Controller, you will need to first select the Panel description from the pull-down list as shown above.

After selecting the Panel to administrate, you could click on any hyperlink to the items that you want to configure.

Once you click on any of the hyperlink as described above, the page showing the selected function will appear for the selected Panel.

16.2 How to Setup Access Groups

An *Access Group* defines a list of Readers within certain authorised time periods (pre-defined Schedule) that the cardholders can access. This means that only within this Schedule, cardholders with this access group can access this Reader. There are 254 programmable Access Groups.

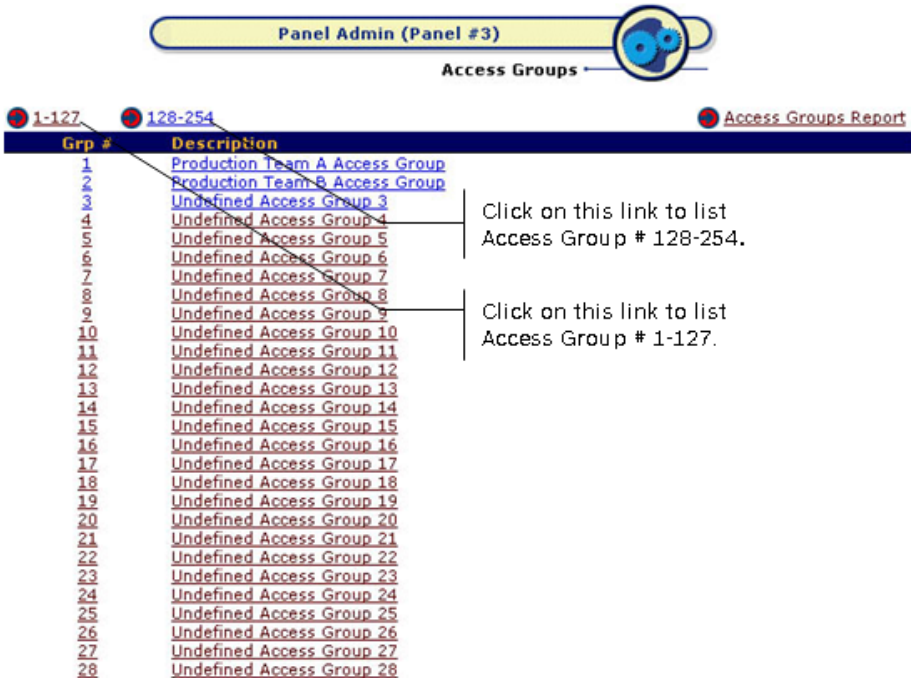
In addition, there are two more unique *Access Groups*. They are the *Full Access* group that allows cardholders to access all Readers at all times, usually reserved for the President, Chairman or Directors of the company and the *Unused* group that prohibits cardholder to access any Reader at any time. These 2 Access Groups are not listed in the Access Groups page. They can be selected when the user goes to Access Levels page.

Access Group is implemented to simplify the process of assigning cardholder's access rights to each Reader. Usually a group of cardholders can access the same group of Readers and usually using a common Schedule. Rather than assigning each Reader to one of the cardholder and going through the same steps repeatedly, grouping of *Access Group* is implemented.

It is highly recommended that detail planning be done before setting up the *Access Groups*.

Each *Access Group* can configure up to 16 Readers with each Reader linked to a Schedule.

To Setup the *Access Groups*, select the target Access Easy Controller and click on the *Access Groups* hyperlink. The following screen will appear.

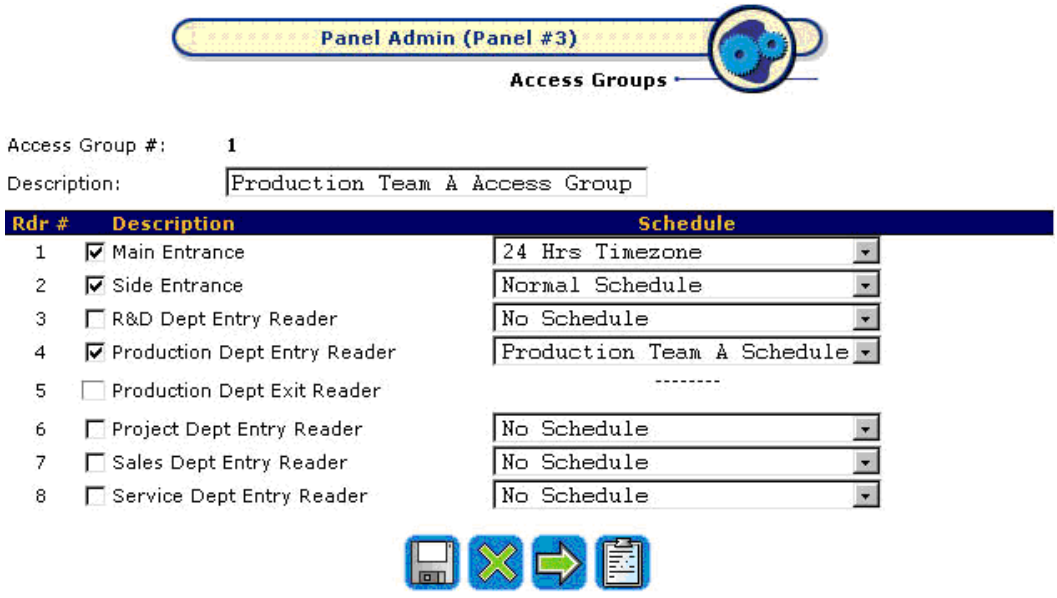

Panel Admin (Panel #3)
Access Groups
1-127
128-254
Access Groups Report
Grp #
Description
1 Production Team A Access Group
2 Production Team B Access Group
3 Undefined Access Group 3
4 Undefined Access Group 4
5 Undefined Access Group 5
6 Undefined Access Group 6
7 Undefined Access Group 7
8 Undefined Access Group 8
9 Undefined Access Group 9
10 Undefined Access Group 10
11 Undefined Access Group 11
12 Undefined Access Group 12
13 Undefined Access Group 13
14 Undefined Access Group 14
15 Undefined Access Group 15
16 Undefined Access Group 16
17 Undefined Access Group 17
18 Undefined Access Group 18
19 Undefined Access Group 19
20 Undefined Access Group 20
21 Undefined Access Group 21
22 Undefined Access Group 22
23 Undefined Access Group 23
24 Undefined Access Group 24
25 Undefined Access Group 25
26 Undefined Access Group 26
27 Undefined Access Group 27
28 Undefined Access Group 28
Click on this link to list Access Group # 128-254.
Click on this link to list Access Group # 1-127.

1. Click on the 1-127 or 128-254 link to list the appropriate Access Groups ranges.

   Alternatively, you can click on the button to go to 128-254 range listings or the button to go to the 1-127 range listings.

16.2.1 How to Configure/Edit Access Group parameters

1. Click on the *Grp #* or the *Description* text to proceed. A screen as shown below appears.


Panel Admin (Panel #3)
Access Groups
Access Group #: 1
Description: Production Team A Access Group
Rdr # Description Schedule
1 Main Entrance 24 Hrs Timezone
2 Side Entrance Normal Schedule
3 R&D Dept Entry Reader No Schedule
4 Production Dept Entry Reader Production Team A Schedule
5 Production Dept Exit Reader --------
6 Project Dept Entry Reader No Schedule
7 Sales Dept Entry Reader No Schedule
8 Service Dept Entry Reader No Schedule

NOTICE!

The Reader's *Description* shown above is configured in *Card Readers* setting. Please refer to *Card Readers* for details.

Reader #5 is configured as Exit Reader for the Production Department. Its operational behaviour will follow that of the Entry Reader and thus no Schedule can be configured.

2. Delete the default text and enter the new *Description*.
3. Click on the appropriate check boxes to indicate a tick mark, for Reader(s) to be assigned to this *Access Group*.
4. Select the appropriate Schedule from the list for each selected Reader.

NOTICE!

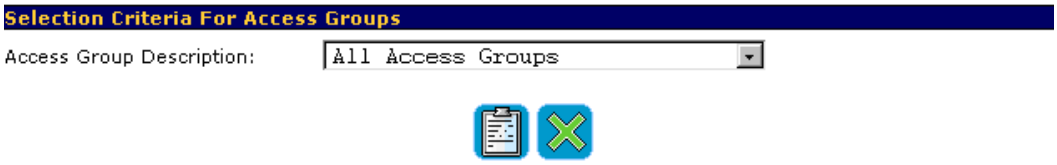
The above example shows that Staff from Production Department Team A can have 24 hours access to the Main Entrance and access to their own department according to their work shift. In addition, other than the normal work hours, they are not allowed to come in by the Side Entrance as its Schedule is not 24 hours access.

5. If you have completed the settings for the first 8 Readers, proceed to the next 8 Readers (only if required) by clicking on the button. Repeat steps 3 and 4.
6. To confirm the setting, click on button.

16.2.2 How to Generate a Print Preview of the Access Groups Report

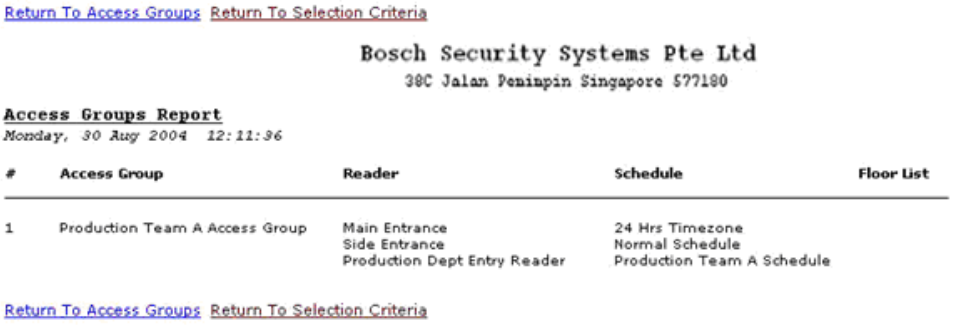
Once you have completed configuring the required Access Groups, a hardcopy can be printed out. To print any one or all Access Groups Report, select from the list box.

1. From the first web page of the Access Groups menu item, click on the Access Groups Report link. A screen as shown below appears.



2. Select the desired Access Group from the drop-down list. If no particular Access Group is selected, all the available Access Groups will be generated in the report.
3. Click on the button for a print preview of the report.

The following screen-capture shows a sample of the Access Groups Report for Production Team A Access Group.


Return To Access Groups Return To Selection Criteria
Bosch Security Systems Pte Ltd
30C Jalan Pemimpin Singapore 577180
Access Groups Report
Monday, 30 Aug 2004 12:11:36
Access Group Reader Schedule Floor List
1 Production Team A Access Group Main Entrance 24 Hrs Timezone
Side Entrance Normal Schedule
Production Dept Entry Reader Production Team A Schedule
Return To Access Groups Return To Selection Criteria

NOTICE!
All Access Groups are available for selection. However, Access Groups that are not defined with at least a Reader will generate an empty report.

If you are satisfied with the configuration and wish to print out a hardcopy, click on the Print button located on the Toolbar of the web browser program. Alternatively, click on the *File* and select *Print*.

4. To return to the Selection Criteria, click on the Return To Selection Criteria link.
5. To return to the Access Groups first web page, click on the Return To Access Groups link.

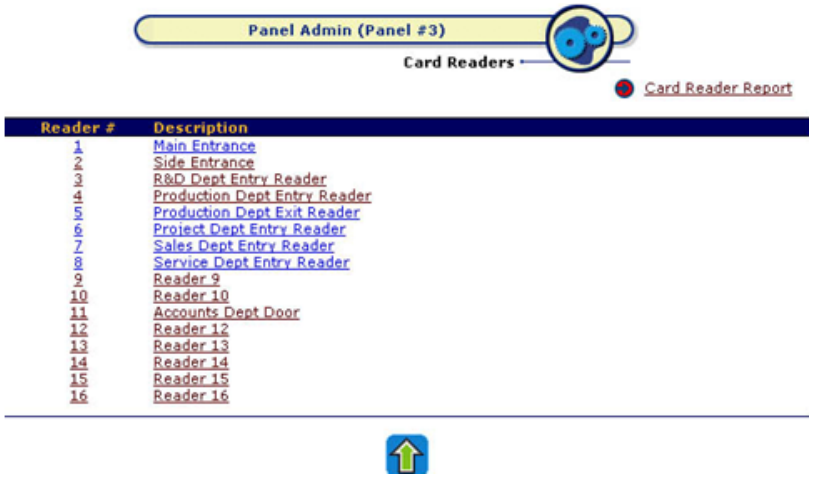
16.3 How to Setup Card Readers

Card Readers parameters are the most essential parameters, comprising of:-

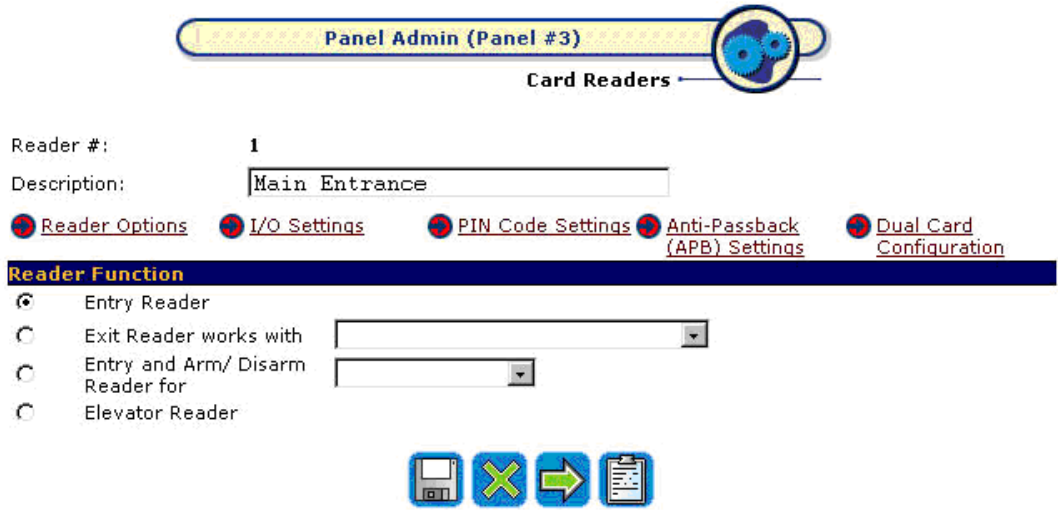
- Reader Function
- Reader Options
- I/O Settings
- PIN Code Settings
- Anti-Passback (APB) Settings
- Dual Card Configuration

All Access Easy Controller Card Readers can be configured to work either as an Entry Reader, an Exit Reader, an Entry and Arm/Disarm Reader or an Elevator Reader.

To Setup the Card Readers, select the target Access Easy Controller and click on the *Card Readers* hyperlink. The following screen will appear.

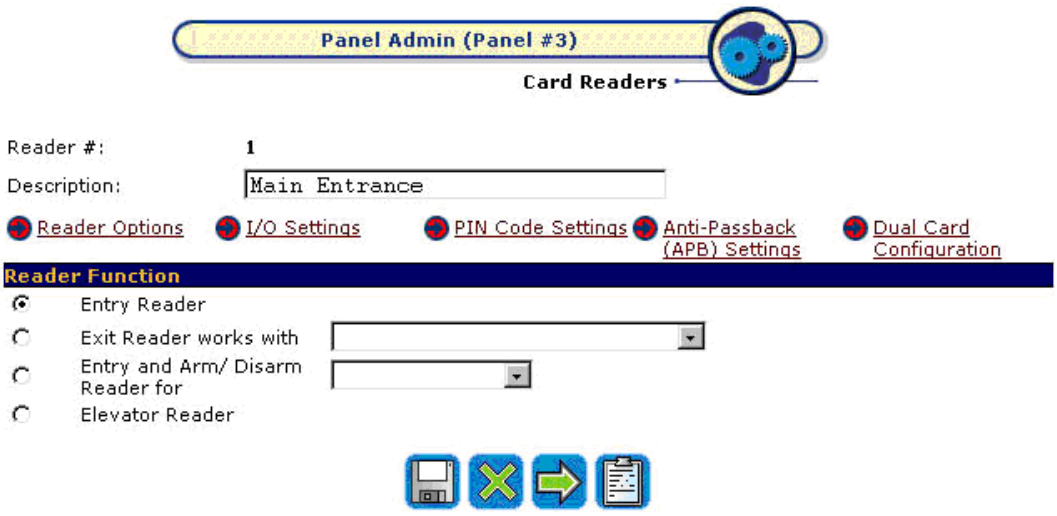


1. Click on the *Reader #* or the *Description* text to proceed. A screen as shown below appears.



2. Delete the default text and enter the new *Description* for the Reader.
3. Click on the button.

16.3.1 Reader Function

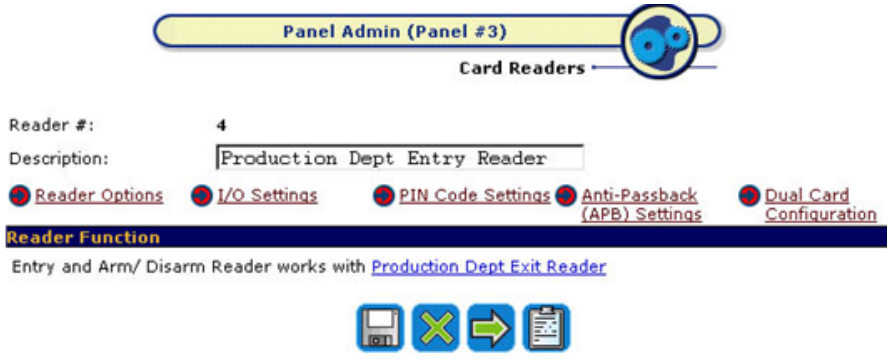


This section allows user to define the use of the Reader, either an Entry Reader, an Exit Reader, an Entry and Arm/Disarm Reader or an Elevator Reader. By default, all 16 Readers are set as Entry Reader.

A screen of the *Reader Function* page is shown above.

Entry Reader
This is the default setting. All 16 readers are configured as Entry Reader allowing Door Access.

If an Entry Reader is defined to work with an Exit Reader, the Reader Function for the Entry Reader will change to reflect the status. A sample is shown in the screenshot below. The Exit Reader's description becomes a hyperlink. User can click on it to re-configure the Exit Reader



Exit Reader
When this mode is selected, this Reader will operate as an Exit Reader.
User has to define the Entry Reader that this Exit Reader has to work with.

This Exit Reader will follow the operational behaviour of the Entry Reader such as Door Open Timer and Door Strike Timer. If the Entry Reader for this Exit Reader is also a Arm/Disarm Reader, user can also arm/disarm the same Alarm Zone at the Exit Reader as it now has the operational behaviour of the Entry Reader.

NOTICE!
Once a Reader is configured as an Exit Reader, the Reader will only be accessible to Reader Functions. The rest of the configuration, such as R*eader Options, I/O Settings, PIN Code Settings, Anti-Passback (APB) Settings* and *Dual Card Configuration* will not be available until it is changed to an Entry Reader, or an Entry and Arm/Disarm Reader.

Entry and Arm/Disarm Reader
When this mode is selected, this Reader will have all the functions of an Entry Reader and it can be used for Arming and Disarming a specific Alarm Zone, i.e. this Reader can be used for door access control and it can also be used to perform Alarm Zone Arm/Disarm function.

To arm an Alarm Zone using the same access Reader, card holder with the Arm/Disarm control just has to press the <0> key on the Keypad before presenting his card.

During an Arm state, all valid access card will be disabled. Only a Arm/Disarm card (*Card must be checked at Card holder is able to Arm/Disarm under Card Assignment.*) can disarm the Alarm Zone and enable the door back to normal card access operation.

During Arm state, if the door is unlocked by Schedule or manually from Door control page, the alarm zone will be disarmed first before door is unlocked.

If the Reader is only used for Arm/Disarm purpose, user just has to assign the cardholder with Arm/Disarm function without given access right to the Reader. This will allow the cardholder to arm the Alarm Zone without pressing the <0> key.

To switch the Reader back to normal access card Reader, press <0> on the Keypad after finishing the Arm/Disarm operation.

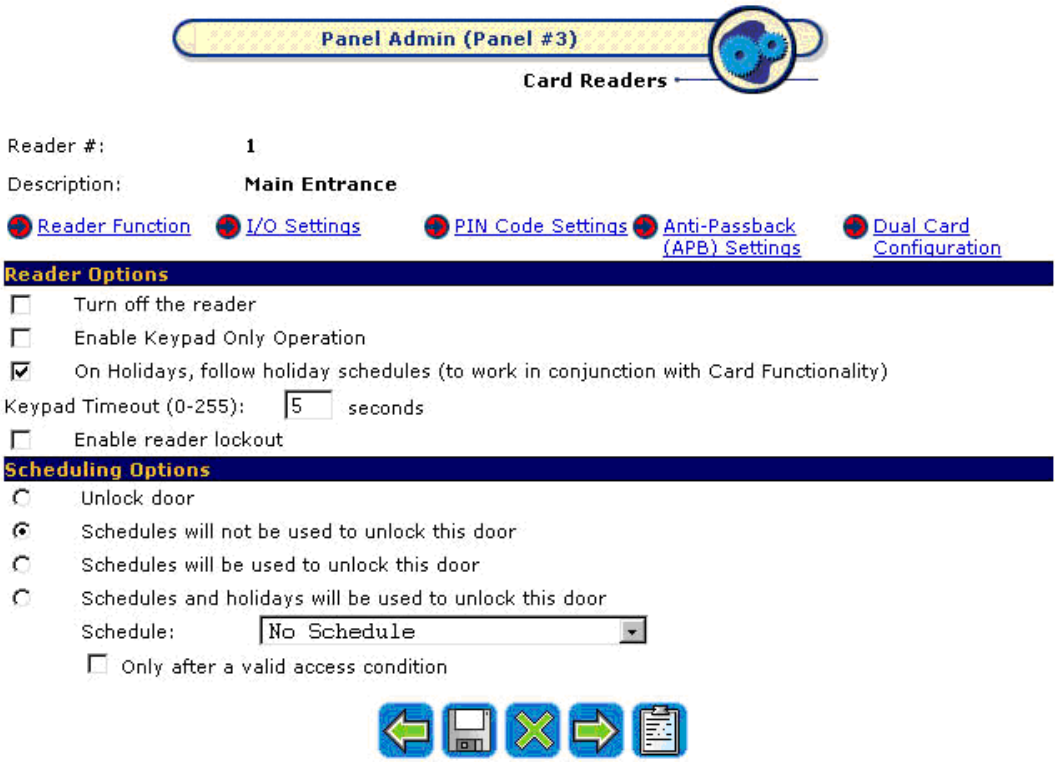
NOTICE!
In order for the Reader to work properly, additional wiring is required. Please consult your System Installer for advice.

Elevator Reader
Similar concept of door access right assignment in other Readers is also implemented in the *Elevator Reader* floor assignment.

However, *Elevator Readers* do not have the function *Anti-Passback (APB) Settings*. This is because it would be complicated to register a zone for the user after he has entered the elevator and flashed his card to the Elevator Reader, since the elevator has exit to more than one floor (You can consider the Elevator has more than one exit).

Besides without the function Anti-Passback (APB) Settings, the *I/O Settings* of *Elevator Reader* is also different from that of an *Entry Reader* and *an Entry and Arm/Disarm Reader*. Elevator Reader only has *Floor Output Settings* and *Output Link*, compared to the *Door Output Settings*, *Door Input Settings* and *Output Link* in Entry Reader, and Entry and Arm/Disarm Reader. The *Output Link* is also reduced to controlling *Invalid Card Output* only in an Elevator Reader

16.3.2 Reader Options


Panel Admin (Panel #3)
Card Readers
Reader #: 1
Description: Main Entrance
Reader Function
I/O Settings
PIN Code Settings
Anti-Passback (APB) Settings
Dual Card Configuration
Reader Options
Turn off the reader
Enable Keypad Only Operation
On Holidays, follow holiday schedules (to work in conjunction with Card Functionality)
Keypad Timeout (0-255): 5 seconds
Enable reader lockout
Scheduling Options
Unlock door
Schedules will not be used to unlock this door
Schedules will be used to unlock this door
Schedules and holidays will be used to unlock this door
Schedule: No Schedule
Only after a valid access condition

This section allows user to configure parameters in relation to the Reader. User can de-activate the Reader to prevent access by anyone, or allow access by entering the Card Number manually, and/or access in accordance to Holiday Schedules.

A screen of the *Reader Options* page is shown above.

Turn off the reader

Once a Reader is turned off, it will not read any card. The door will be locked and all access will be denied. For Arm/Disarm Reader, turning off the reader prevents arming and disarming through the Reader.

Enable Keypad Only Operation

When this mode is selected, the user need not present his/her card to gain access or Arm/Disarm the Alarm Zone (see NOTICE 1). Instead, the cardholder only has to key in his/her card number, (see NOTICE 2) followed by its PIN code (Only if PIN function is required).

NOTICE!

1. Cardholder can still present his/her card to gain access or Arm/Disarm. If PIN code is required, user has to present card followed by PIN code.
2. User has to activate the

key first before entering the card number.

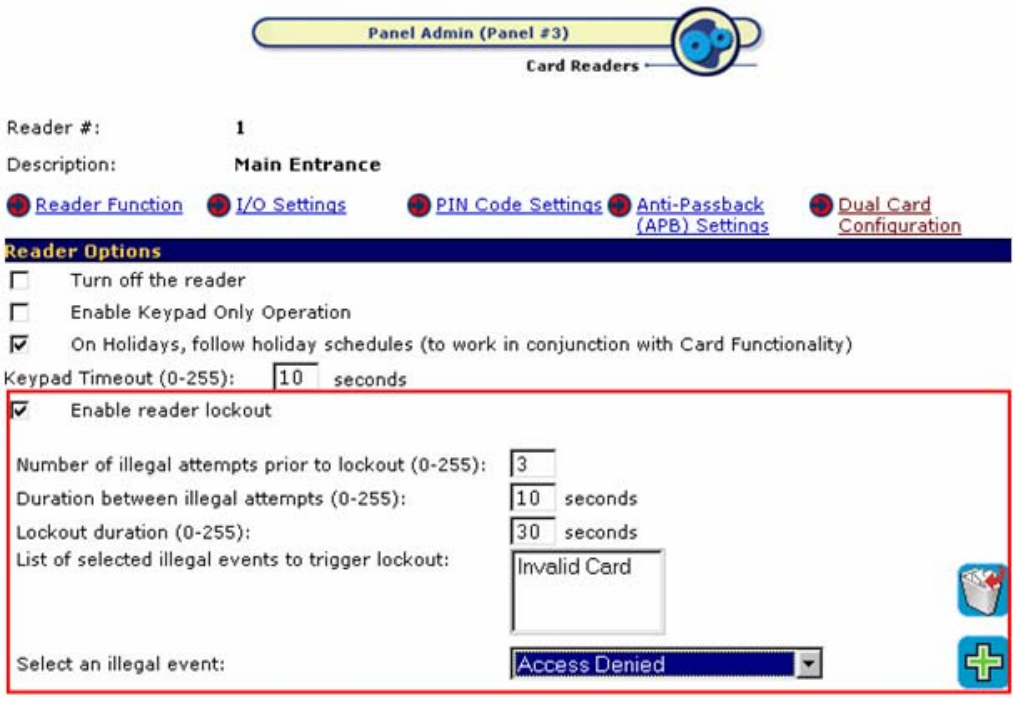
On Holidays, follow holiday schedules (to work in conjunction with Card Functionality)
This mode works in conjunction with the *Card Assignment, Cardholder must abide by holiday schedules.* If both are checked and the current date is a holiday, the panel will apply the 4 sets of Schedule intervals setting in the Regular or Special Holiday, depending on which Holiday Type the current date setting is on, for processing (for each cardholder).

Keypad Timeout
Keypad Timeout relates to the interval where the Panel expects key entry via the reader's keypad from the user. If the user does not press any key within this duration or when the user forgets to quit from a specific operation, the Panel will return to the normal mode to wait for card presentation or user action during a PIN change or Manual Card Number Entry operation. To edit the Keypad Timeout, delete the default number and enter the new timeout value. It should range from 0 - 255. The factory default is 10 seconds.

Enable Reader Lockout

When this mode is selected, there is a restriction on the number of times a user with invalid access can present his card at the Reader.

1. Check on the *Enable Reader Lockout* and click on the button. A screen as shown below appears.


Panel Admin (Panel #3)
Card Readers
Reader #: 1
Description: Main Entrance
Reader Function
I/O Settings
PIN Code Settings
Anti-Passback (APB) Settings
Dual Card Configuration
Reader Options
Turn off the reader
Enable Keypad Only Operation
On Holidays, follow holiday schedules (to work in conjunction with Card Functionality)
Keypad Timeout (0-255): 10 seconds
Enable reader lockout
Number of illegal attempts prior to lockout (0-255): 3
Duration between illegal attempts (0-255): 10 seconds
Lockout duration (0-255): 30 seconds
List of selected illegal events to trigger lockout:
Invalid Card
Select an illegal event:
Access Denied

2. Choose the events that you would like to lock the users out by selecting from *Select an illegal event* and click on the button.
3. The illegal events will appear on the *List of selected illegal events to trigger lockout*.

4. To remove the illegal event from the *List of selected illegal events to trigger lockout*, highlight the event and click on the button.
5. Enter the *Number of illegal attempts prior to lockout*. The default is set to 3.
6. Enter the *Duration between illegal attempts*. It ranges from 0 to 255 seconds.
7. Enter the *Lockout duration*. It ranges from 0 to 255 seconds.

In the above example, the user will be lockout after the 3rd attempt when he uses an Invalid Card to access the Reader 3 times within 10 seconds. He would not be able to access the Reader for 30 seconds, meaning the Reader will lock him out for 30 seconds. However, if he only attempted 2 times with an invalid card, the Reader will reset the illegal attempt counter 10 seconds after the very first time the user uses an invalid card to access the Reader.

NOTICE!
Once Reader is lockout, it will not be accessible by any cardholder. Only after the lockout duration can the reader be used again.

16.3.3 Scheduling Options

The Access Easy Controller can be programmed to activate or de-activate the reader based on pre-programmed Schedules. This is particularly useful if the reader is used for controlling door access and the door is required to be unlocked during certain period of the day, but to be locked back at different time period for the same day.
The above scenario is a typical operation of a Main Entrance Door of a building. During the time when staff normally come to work, you might want to unlock the door throughout the office working hours and automatically lock back after work.

A screen of the *Scheduling Options* page is shown in the section Reader Options.

Unlock door (For Entry Reader, Entry and Arm/Disarm Reader)
When this mode is selected, the door that is controlled by the particular reader is permanently unlocked. There is free access to everyone. This function is applicable to Entry Reader, and Entry and Arm/Disarm Reader ○ Unlock door. For Elevator Reader, this function is replaced by a similar function *Disable Elevator Reader*, in the below section.

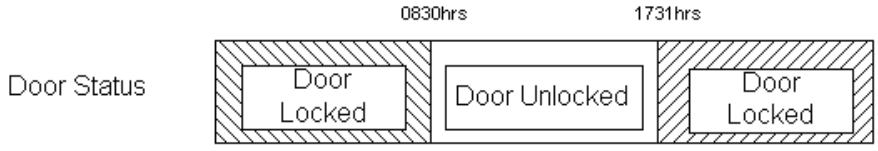
Disable Elevator Reader (For Elevator Reader Only)
When this mode is selected, the elevator that is controlled by the particular reader is permanently unlocked. There is free access to everyone. This function is applicable to Elevator Reader only ○ Disable Elevator Reader. For Entry Reader, and Entry and Arm/Disarm Reader, it is replaced by a similar function *Unlock door*, in the above section.

Schedules will not be used to unlock this door
When this mode is selected, the reader access mode will be activated. Gaining access will require the user to present his / her card and PIN code (if PIN code is required).

Schedules will be used to unlock this door

When this mode is selected, the Reader access mode will function based on the Schedule intervals setting. To set the scheduling options, refer to the section on *To set the Scheduling Options* below.

For example: - The Start and End time for Interval 1 of Schedule settings is set to 0830hrs and 1730hrs respectively. In this period, the door will be unlocked between 0830 to 1731 hrs. The drawing below provides a pictorial representation of the function.



Notice that the Door is locked only at 1731hrs instead of 1730hrs. The reason is that Access Easy Controller takes 17:30:59hrs as a valid End time for 1730hrs.

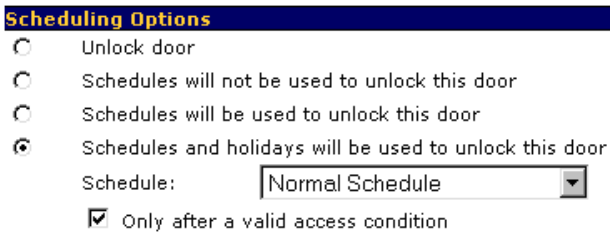
Schedules and Holidays will be used to unlock this door

When this mode is selected, during a Holiday, the Cardholder will be allowed to access this Reader during the specific period as defined in Schedule intervals setting for holiday. To set the scheduling options, refer to the section on *To set the Scheduling Options* below.

To set the Scheduling Options (For Schedules will be used to unlock this door and Schedules and Holidays will be used to unlock this door)

1. To assign the *Scheduling Options*, click on the desired radio button. To de-select that point, click on other radio buttons. By default, it is set at *Schedules will not be used to unlock this door*.
2. If the selection is made on either Schedules will be used to unlock this door or Schedules and Holidays will be used to unlock this door, please proceed to step 3 to select the Schedule.
3. Select the desired *Schedule* from the *Schedule* list box.
4. When *Schedules will be used to unlock this door* or *Schedules and Holidays will be used to unlock this door is selected*, the door will unlock on time even if nobody is in the premises. However, with the *Only after a valid access condition* checked, the system will only unlock the door after a valid access card is presented during the schedule time period.

   Example


Scheduling Options
Unlock door
Schedules will not be used to unlock this door
Schedules will be used to unlock this door
Schedules and holidays will be used to unlock this door
Schedule:
Normal Schedule
Only after a valid access condition

In the screen above, the mode *Schedules and Holidays will be used to unlock this door* is selected, and the selected *Schedule* is Normal Schedule. In addition, the checkbox *Only after a valid access condition* is checked.

The screen below shows the schedule for 'Normal Schedule', which has been selected.

Schedule #: **4**

Schedule Description: Normal Schedule

		Interval 1		Interval 2		Interval 3		Interval 4	
		Start	End	Start	End	Start	End	Start	End
Sunday		08:30	13:00	--:--	--:--	--:--	--:--	--:--	--:--
Monday		08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
Tuesday		08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
Wednesday		08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
Thursday		08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
Friday		08:30	17:30	--:--	--:--	--:--	--:--	--:--	--:--
Saturday		08:30	13:00	--:--	--:--	--:--	--:--	--:--	--:--
Regular Hol		08:30	13:00	--:--	--:--	--:--	--:--	--:--	--:--
Special Hol		08:30	13:00	--:--	--:--	--:--	--:--	--:--	--:--

According to the schedule in 'Normal Schedule' above, when the mode *Schedules and Holidays will be used to unlock this door* is selected, the door will unlock every Monday to Friday from 0830hrs to 1730hrs and every Saturday, Sunday, Regular Holiday and Special Holiday from 0830hrs to 1300hrs. However, with *Only after a valid access condition* is checked, the door will only unlock after a valid access card is presented to the Reader during the schedule time period. For example, on a Monday, the first person to present his card to the Reader arrives at 0845hrs. Therefore, the door will only unlock from 0845hrs to 1730hrs on that particular Monday, instead of from 0830hrs to 1730hrs.

16.3.4 Door Output Settings (For Entry Reader, Entry and Arm/Disarm Reader)

This parameter allows user to set the timer duration that is related to the door.

A screen of the *Door Output Settings* page is shown above.

Door Open Timer
This setting defines how long the door can be held open, after an access/exit is granted, before the Panel registers it as Door Held Open transaction. If the reader has a built-in buzzer, it will generate a beeping alert signal and will stop once the door is closed back. It can range from 0 to 255 seconds. The factory default is 60 seconds.

Door Strike Timer
This setting defines the duration to de-energise the Door Strike when the Momentarily Unlock command is sent via the Door Control web page or when an access/exit is granted.
When access is granted to a Cardholder, sufficient time must be given for the person to open the door before the Panel locks it back again. It can range from 0 to 255 seconds. The factory default is 5 seconds.

NOTICE!
When the Door Strike Timer is set to 0, and a valid card is presented at the Reader, the door becomes unlocked (View Activity shows Door Unlocked) until the same card or another valid card is presented at the Reader, only then the Reader will go back to locked mode (View Activity shows Door Locked). Presenting an invalid card will not change the status. View Acivity will only show Invalid Card.

Door Strike
For the Output device, such as Door Strike, though it is pre-defined, user can still change the default address to other available addresses within the same Reader board, should the original output relay is defective.

To allocate an Output Address for *Door Strike*, select *Output* for *Source*, else select *None*. *After allocating Output* to *Source*, select an *Address* for it. The default Address is 1. The *Address* can be chosen from a selectable range.

Output
It defines the physical output on the Reader board. The output channels are applicable for *Door Strike, Door Forced Alarm Output, Door Held Alarm Output* and *Invalid Card Output*. Output channel assignment for devices connected in relation to the Reader is selectable within the spare Output channels of the card. User can disable the Output channel by selecting None.

None
This setting will disable the Output channel.

NOTICE!
Address for *Door Strike* is selectable only to within the Card's spare Output channels. *Door Forced Alarm Output, Door Held Alarm Output* and *Invalid Card Output* is selectable only within the user programmable 32 outputs.

16.3.5 Door Input Settings (For Entry Reader, Entry and Arm/Disarm Reader)

A screen of the *Door Input Settings* page is shown in the section *Door Output Settings*.

The Access Easy Controller has the capability to support a maximum of 16 wiegand card readers, 64 input (I) monitoring points, and 64 relay output (O) points.Of the 64 I/Os, only 32 Inputs and Outputs are user programmable, the other 32 I/Os are assigned to the Readers.

The addresses for Input devices (Request-to-Exit device and Door Contact) connected in relation to the Reader, are pre-defined and cannot be changed. The following is the list of hardware to configure: -

- Request-to-Exit Device,
- Door Contact,
- Door Forced Open Alarm delay duration,
- Pre-alarm Warning before door held open alarm.

Request-to-Exit Device
To allocate an Input Address for Request-to-Exit Device, select Input, else select None. The Address for Request-to-Exit Device is fixed and cannot be changed.

Door Contact
To allocate an Input Address for Door Contact, select *Input* for Source, else select *None*. The Address for Door Contact is fixed and cannot be changed.

Input
It defines the physical input on the Reader board. The input channels are applicable to *Request-to-Exit device* and *Door Contact*. Input channel assignment for devices connected in relation to Reader is fixed and cannot be changed. However, user can disable the Input channel by selecting None.

None
This setting will disable the Input channel.

If the door contact is ignored, there will not be any alarms like "Door Held Open" or "Door Forced Open" on that particular reader.

Schedules and holidays will be used to shunt door contact
An additional feature is the enabling schedules and holidays to be used for shunt door contact.

If a schedule is selected, during the time interval, the door contact will be ignored. This is the same as setting the door contact to "None".

If the door contact is ignored, there will not be any alarms like "Door Held Open" or "Door Forced Open" on that particular reader.

Door Forced Open Alarm delay duration
This is to facilitate some special exit requirement. For example, a handicap user will need a longer time to access the open door than a normal user does. This can also be used to prevent Door Forced Open false alarm due to interference at the cables.

Enter the timing in seconds at the Door Forced Open Alarm delay duration if desired. The timing can range from 0 to 255 seconds.

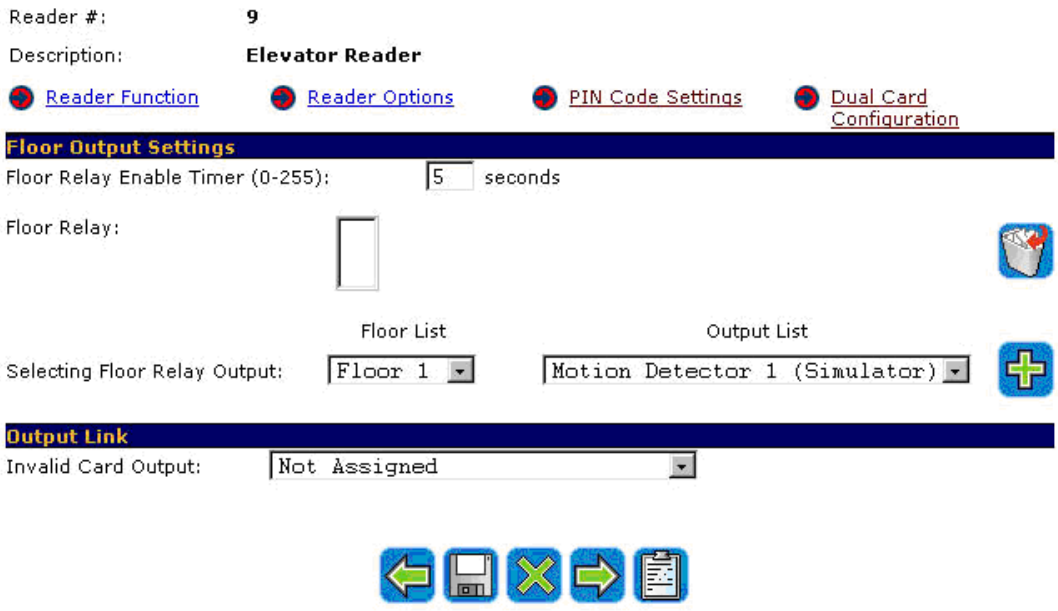
Pre-alarm Warning before door held open alarm
With the pre-alarm function, a user would be reminded with a slow beeping that the door he has just gained access is still open. An example is he can set *Pre-alarm Warning before door held open alarm* to 5 seconds so that he will be alerted to close the door on time before the Door Held Open Alarm. The timing can range from 0 to 60 seconds.

NOTICE!
Address for Request-to-Exit Device and Door Contact is fixed and cannot be changed. If the Input channel is disabled, the address will not be shown.

16.3.6 Floor Output Settings (For Elevator Reader Only)

When a reader is enable as a elevator reader, it will not have any door input or output setting. Instead it will be replaced by floor output settings.

A screen of the *Floor Output Settings* page is shown below.

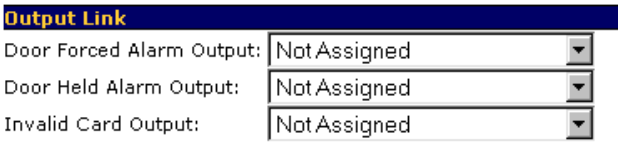


This section allows user to set any of the 32 programmable Output Point to the selected Floor.

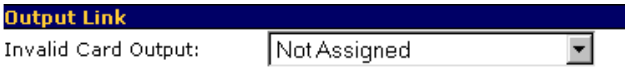
1. To configure the *Selecting Floor Relay Output*, select a Floor from the *Floor List*.
2. Select an Output Point from the *Output List*.
3. Click on the button to add the selected Output Point to the selected Floor. The selected items would appear on the Floor Relay list box, as shown below. Each Floor and Output Point can only be selected once.

4. To delete any selected items from the Floor Relay list box, highlight the item and click on the button.
5. To configure the *Floor Relay Enable Timer*, delete the default timing in seconds and enter a new timing for it. The default timing is 5 seconds.

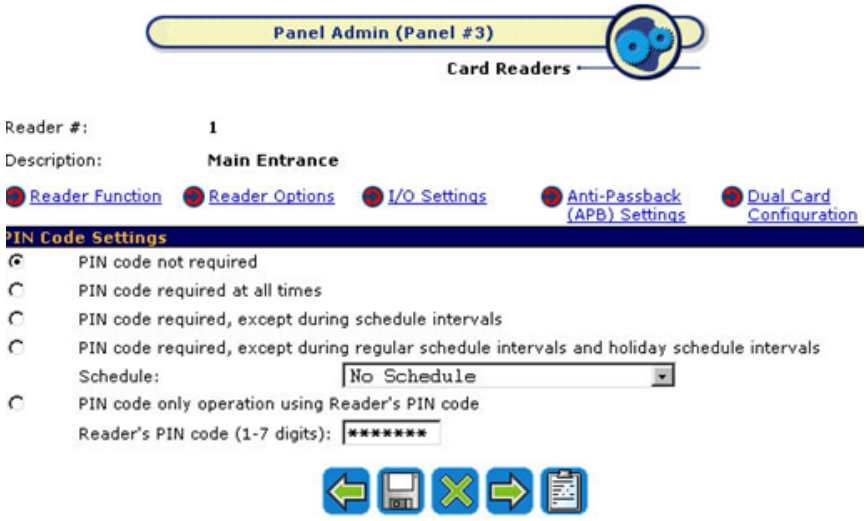
In an Entry Reader, and Entry and Arm/Disarm Reader, it allows user to set any of the 32 programmable Output Point to *Door Forced Alarm Output, Door Held Alarm Output* and *Invalid Card Output*. By default, all the 3 are set to *Not Assigned*.



However, in an Elevator Reader, this section only allows user to set any of the 32 programmable Output Point to *Invalid Card Output*. By default, it is set to *Not Assigned*.



16.3.7 PIN Code Settings


Panel Admin (Panel #3)
Card Readers
Reader #: 1
Description: Main Entrance
Reader Function
Reader Options
I/O Settings
Anti-Passback (APB) Settings
Dual Card Configuration
PIN Code Settings
PIN code not required
PIN code required at all times
PIN code required, except during schedule intervals
PIN code required, except during regular schedule intervals and holiday schedule intervals
Schedule: No Schedule
PIN code only operation using Reader's PIN code
Reader's PIN code (1-7 digits): *******

This section allows user to set the parameter on when the Personal Identification Number (PIN) is to be used.

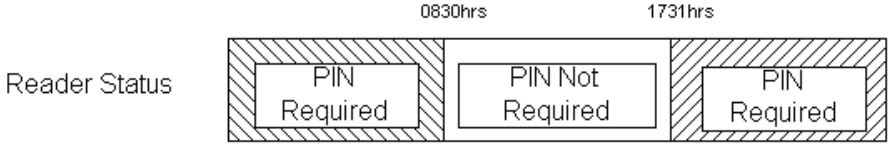
A screen of the *PIN Code Settings* page is shown above.

PIN code not required
When this mode is selected, users accessing this Reader do not have to key in the PIN code.

PIN code required at all times
When this mode is selected, users are required to key in the PIN code.

NOTICE!
In order for the feature to work, the *Cardholder's Card + PIN is required on keypad* readers mode must be activated, and the PIN must be set at the card in Card Assignment page. For the setting of the PIN, please refer to *Chapter 6 Card Assignment, Card Functionality, Card + PIN is required on Keypad readers*.

PIN code required, except during schedule intervals
When this mode is selected, users are not required to key in his/her PIN code during specific periods defined in the Schedule settings.
As an example, the Start and End time for Interval 1 of the Schedule is set to 0830hrs and 1730hrs respectively. The Reader status will be set accordingly. The following drawing provides a pictorial representation of the function.



Notice that PIN is required at 1731hrs instead of 1730hrs. The reason is that Access Easy Controller takes 17:30:59hrs as a valid End time for 1730hrs.

This mode is not affected by Holiday setting, i.e. during holiday, it will still use the Day of Week schedule.

NOTICE!
1. To use this feature as intended, the cardholder should be given access rights to the reader(s).
2. In order for the feature to work, the cardholder's *Card + PIN is required on keypad readers* mode must be activated.

PIN code required, except during regular schedule intervals and holiday schedule intervals
When this mode is selected, the operation is the same as the previous mode, except that during holiday the Holiday schedule is used instead of the normal Day of Week schedule.

PIN code only operation using Reader's PIN code
When this mode is selected, all cardholders will use a pre-defined Reader's PIN code (default code 1234000) to gain access to the controlled area or to arm/disarm the Alarm Zone. No card is required.

The Reader's PIN code is defined in the *Reader's PIN code (1-7 digits)* edit field.

To set the Schedule

1. If selection is made on PIN code required, except during schedule intervals or PIN code required, except during regular schedule intervals and holiday schedule intervals, the Schedule field must be set.
2. To edit the Schedule, select the appropriate schedule from the *Schedule* list box.

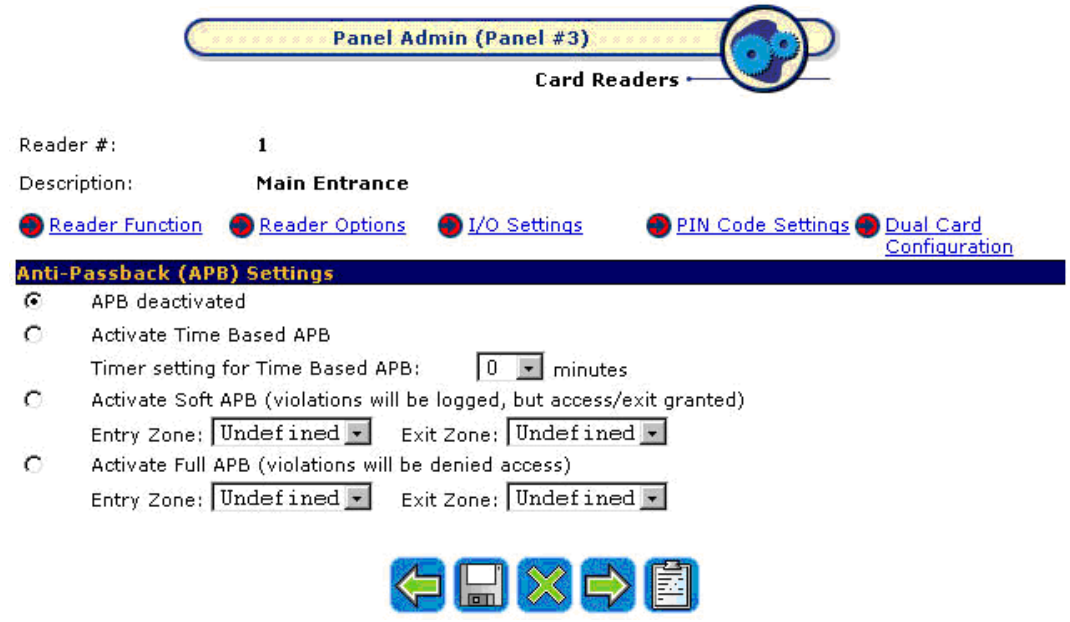
To set the Reader's PIN Code

1. If the selection is made on *PIN code only operation using Reader's PIN code*, the *Reader's PIN code (1-7 digits)* field must be entered.
2. To edit the *Reader's PIN code*, delete the default PIN and enter the new *Reader's PIN code*, limited to 7 digits. See NOTICE 1 And 2.

NOTICE!

1. User can enter from 1 to 7 digits for the Reader's PIN code (default code 1234000).
2. For security reason, every character entered for the PIN code is represented by an asterisk . For Macintosh user, it is represented by a dot instead.

16.3.8 Anti-Passback (APB) Settings


Panel Admin (Panel #3)
Card Readers
Reader #: 1
Description: Main Entrance
Reader Function
Reader Options
I/O Settings
PIN Code Settings
Dual Card Configuration
Anti-Passback (APB) Settings
APB deactivated
Activate Time Based APB
Timer setting for Time Based APB: 0 minutes
Activate Soft APB (violations will be logged, but access/exit granted)
Entry Zone: Undefined Exit Zone: Undefined
Activate Full APB (violations will be denied access)
Entry Zone: Undefined Exit Zone: Undefined

A screen of the *Anti-Passback (APB) Settings* page is shown above.

Anti-Passback (APB) function prevents a cardholder from passing his/her card to another person to gain access to the door after he has accessed through it. It is normally implemented in sensitive area having high security.

Three types of APB modes are available; namely: - Time Based APB, Soft APB, and Full APB. Each mode provides different level of security and is explained in detail in the following sections.

APB deactivated
By default, it is set to *APB deactivated*. This means that there is no APB setting for the Readers on this Access Easy Controller.

Activate Time Based APB
Time Based APB relates to *Entry Reader* only, implying that the Panel will not accept the same card until the Timer setting for Time Based APB has elapsed.

To select this mode, select *Activate Time Based APB*.

When this mode is selected, the *Timer setting for Timed Based APB* must be set. Choose the timing from the list box, in minutes, from a range of 0 minutes to 60 minutes.

Activate Soft APB
Soft APB mode operation requires a cardholder to present his/her card at the *Entry Reader* and *Exit Reader* at all times. However, if he/she follow another person in or out the controlled area, the transaction "Exit Granted, Soft APB" or "Access Granted, Soft APB" will be shown on his/her next exit or entry respectively.
The administrator needs to Reset APB in order to clear the above transaction. Refer to the *Chapter on Reset APB* for detail.

To select this mode, select *Activate Soft APB*. The *Entry Zone* and *Exit Zone* must be selected for this mode to work properly.

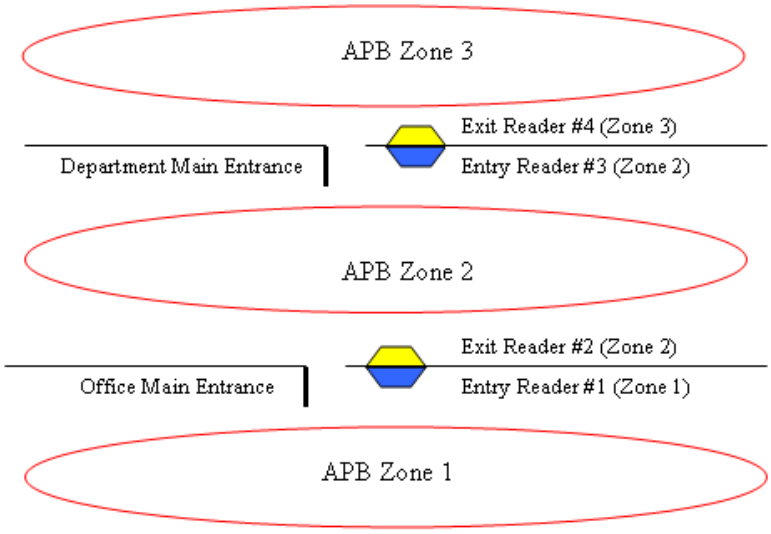
Activate Full APB
When this mode is selected, user must first enter using the *Entry Reader* in order to exit from the corresponding *Exit Reader*. If cardholder violates this, access will be denied. The administrator needs to *Reset APB* before the cardholder can have access again. Refer to the *Chapter on Reset APB* for detail.

To select this mode, select *Activate Full APB*. The *Entry Zone* and *Exit Zone* must be selected for this mode to work properly.

The main difference between the Soft and Full APB is that, for Soft APB, the user is allowed to exit the controlled area via the Exit Reader even if he/she entered the controlled area previously by following another person. Full APB does not allow that.

Understanding the APB Zone

APB Zone is applicable to Soft APB and the Full APB mode.
Access Easy Controller is able to support up to *254 Soft APB Entry Zones, 254 Soft APB Exit Zone, 254 Full APB Entry Zone* and *254 Full APB Exit Zone*.

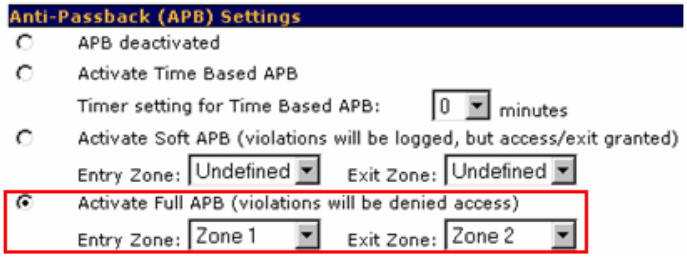


Any Reader assigned to operate Soft APB mode or Full APB mode will be given an *Entry Zone* and *Exit Zone*. When a cardholder presents card at Entry Reader #1, the system will verify whether he has been registered in Zone 1. If he has been registered in Zone 1, access is granted to him. When he opens the door to gain access such that the door contact sensing is opened, he is registered to be in Zone 2. However, if he is verified to be in other zones instead of Zone 1, access will be denied to him.

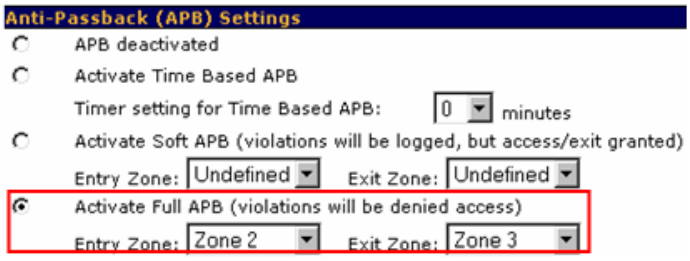
NOTICE!
In the case that he is verified to be in Zone 1 and is granted access but he did not open the door to gain access, he will not be registered in Zone 2. He will only be registered in Zone 2 when he is granted access and opens the door to gain access.

Using this verification method, no card can bypass any zone to gain access to any other zone. In addition, zone will only be registered into the card if the user has opened the door physically (based on door contact sensing).

For the above example, assume that the mode *Activate Full APB (violations will be denied access)* is selected. For Entry Reader #1, the *Entry Zone* will be selected as Zone 1 and *Exit Zone* selected as Zone 2, as shown below.


Anti-Passback (APB) Settings
APB deactivated
Activate Time Based APB
Timer setting for Time Based APB: 0 minutes
Activate Soft APB (violations will be logged, but access/exit granted)
Entry Zone: Undefined Exit Zone: Undefined
Activate Full APB (violations will be denied access)
Entry Zone: Zone 1 Exit Zone: Zone 2

Similarly, for Entry Reader #3, the Entry Zone will be selected as Zone 2 and Exit Zone selected as Zone 3, as shown below.


Anti-Passback (APB) Settings
APB deactivated
Activate Time Based APB
Timer setting for Time Based APB: 0 minutes
Activate Soft APB (violations will be logged, but access/exit granted)
Entry Zone: Undefined Exit Zone: Undefined
Activate Full APB (violations will be denied access)
Entry Zone: Zone 2 Exit Zone: Zone 3

16.3.9 Dual Card Configuration

Panel Admin (Panel #3)
Card Readers
Reader #: 1
Description: Main Entrance
Reader Function
Reader Options
I/O Settings
PIN Code Settings
Anti-Passback (APB) Settings
Dual Card Configuration
Dual Card Mode disabled
After using 2 card to initiate the access, the system will switch back to single card access
Dual Card access at all time

In the *Dual Card Configuration*, the Reader can either be configured as *Dual Card Mode disabled, After using 2 card to initiate the access, the system will switch back to single card access* or *Dual Card access at all time*.

A screen of the Dual Card Configuration page is shown above.

Dual Card Mode disabled
If this mode is selected, it means that no 2 cards are needed to activate the Reader.

After using 2 card to initiate the access, the system will switch back to single card access
If this mode is selected, it means that after 2 cards are presented to the same Reader to unlock the door, the Reader will switch back to single card access.

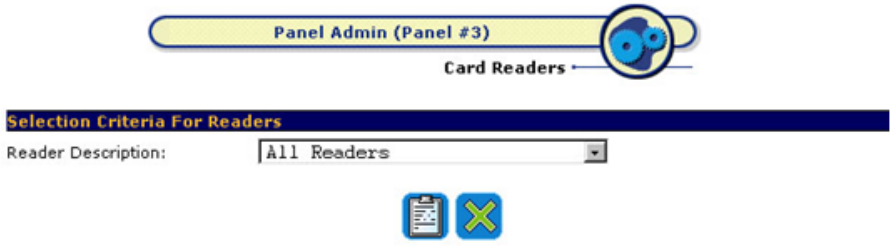
An example of the scenario would be as follows:
In the morning, 2 authorized personnel with dual card function have to present their card at the high security door Reader before the door can be accessed normally. Subsequently the rest of the employees would access the door using their own card. At the end of the day, either of the 2 authorized personnel holding the dual card will have to revert the system back to dual card mode by pressing the <3> key on the Keypad before presenting their cards.

Dual Card access at all time
If this mode is selected, it means that 2 cards have to be presented to the Reader at all times to unlock the door. This mode works in conjunction with the *Dual Card Assignment* under the chapter *Card Assignment* as to whether there is any order in the presentation of cards.

16.3.10 How to generate a Print Preview of the Card Reader Report

Once you have completed configuring the Card Readers, a hardcopy can be printed out.

1. From the first web page of the Card Readers menu item, click on the Card Reader Report link. A screen as shown below appears.



2. Select the desired Reader from the *Reader Description* list box. If no reader is selected, the report generated will include all the available readers in the selected panel. In this example, all the readers in Panel #3 will be included in the report.

3. Click on the button for a print preview of the report.

The following screen-capture shows an example of the report for the Main Entrance.

Return To Card Readers Return To Selection Criteria

Bosch Security Systems Pte Ltd
30C Jalan Pemimpin Singapore 577180

Card Reader Report
Monday, 30 Aug 2004 15:46:06

Reader # : 1
Description : Main Entrance

Reader Function
Entry Reader

Reader Options
Turn off the reader : Not Selected
Enable Keypad Only Operation : Not Selected
On Holidays, follow holiday schedules (to work in conjunction with Card Functionality) : Selected
Keypad Timeout : 5 seconds
Enable reader lockout : Not Selected

Scheduling Options
Schedules will not be used to unlock this door
Only after a valid access condition : Not Selected

Door Output Settings
Door Open Timer : 60 seconds
Door Strike Timer : 5 seconds
Door Strike : Output 1

Door Input Settings
Request-to-Exit Device : Input 1

4. If you wish to view other Reader's configuration, click on the Return To Selection Criteria link and reselect.
   If you are satisfied with the configuration and wish to print out a hardcopy, click on the Print button located on the Toolbar of the web browser program. Alternatively, click on the *File* and select *Print*.

5. To return to the Card Readers first web page, click on the Return To Card Readers link.

16.4 Input Setup

The Access Easy Controller has 32 user programmable Input Points that will be used for Alarm Monitoring purposes. The addresses for these Input Points range from 33 to 64 and are available on the I/O Card. Each card provides up to eight Input Points.

These Input Points can be assigned into a Group (called an Alarm Zone) or as an Individual. Both types provide the same function. The only difference is the way each is being armed/disarmed. Access Easy Controller allows user to configure up to four Alarm Zones.

An Alarm Zone (see NOTICE 2 below) can be armed/disarmed by the following methods: -

- Manually by user via a dedicated Arm/Disarm Reader, or
- Manually by user via the web page (Input Control), or
- System control based on Schedule Intervals.

An Individual Input Point can be armed/disarmed only by Schedule intervals or manually by user via the web page. To arm/disarm an Input Point via the web page, go to *Manual Control, Input Control.*

All Input Points, Group or Individual, can be configured to trigger 1 to 4 Output Points (of the I/O Card) for the purpose of status indication. The Outputs are labelled as: -

Alarm Status	Turns "ON" during an Alarm condition.
Arm/Disarm Status	Turns "ON" when it is Armed.
Ready Status	Turns "ON" when the Input Point is not in the normal condition. It is said to be Not Ready for Arming.
Bypass Status	Turns "ON" when the Input Point is Bypassed.

Any alarm detected by any of the Input Points would also trigger the *Common Alarm Output relay*, at address 8, and is only restored when all the Input Points is restored back to *Normal state.*

NOTICE!

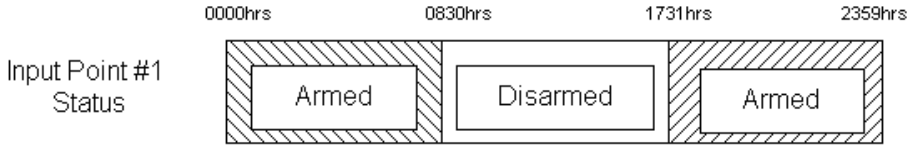
1. The Input Control web page will display the status of the Alarm Zones as well as the status of individual Input Points. Please refer to *Chapter 5 Manual Control, Input Control for detail.*

2. All Input Points configured to an Alarm Zone follow the First Input Point's setting for Arm Delay, Alarm Delay, and Schedule of that Zone.

Before we start, here is a brief description of how the Access Easy Controller interprets the Schedule Intervals for Input Points arming and disarming statuses

For example,
If the setting for Schedule #2 is: -
Interval 1Start 0830hrsEnd 1730hrs
Interval 2, 3, and 4 has no setting.

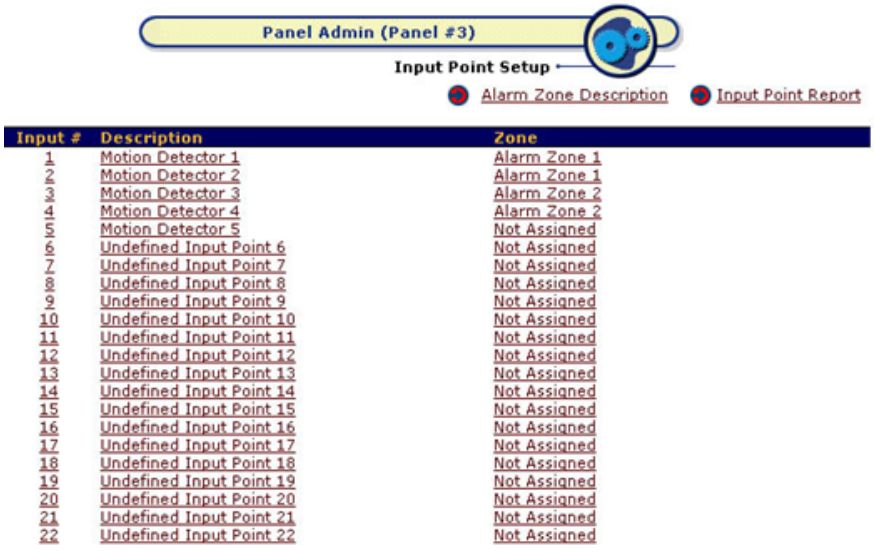
When the Schedule #2 is tied to Input Point #1, the input point will arm and disarm accordingly.



Take note that the Input Point is disarmed at exactly 0830hrs but re-armed at 1731hrs, a minute delay, as compared to the Schedule #2 setting. The reason is that Access Easy Controller takes 17:30:59hrs as a valid End time for 1730hrs.

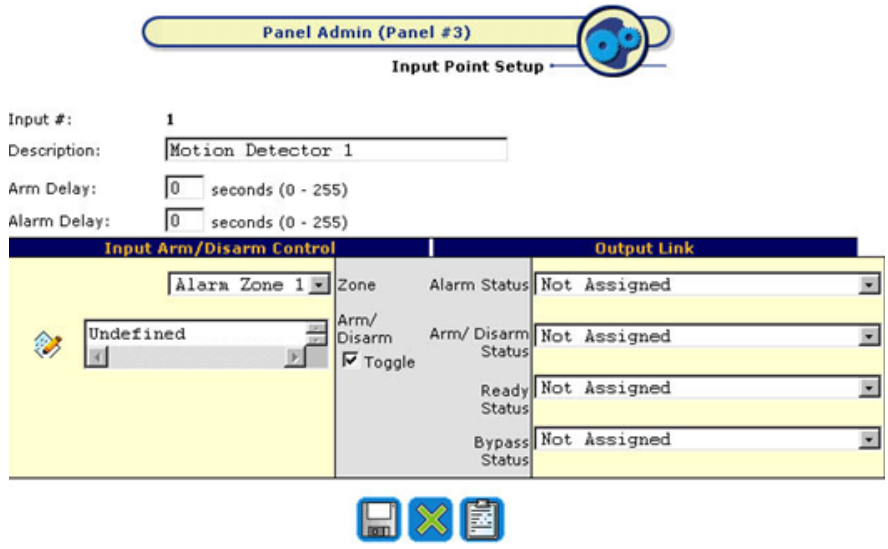
NOTICE!
Before you configure any Input Point(s), please ensure that the Alarm Monitoring Device with the EOL resistor is in place with the necessary logic inversion on the Input Point Configuration web page.

1. To Setup the Input Point select the target Access Easy Controller and click on the *Input Setup hyperlink*. The following screen will appear.



Input #	Description	Zone
1	Motion Detector 1	Alarm Zone 1
2	Motion Detector 2	Alarm Zone 1
3	Motion Detector 3	Alarm Zone 2
4	Motion Detector 4	Alarm Zone 2
5	Motion Detector 5	Not Assigned
6	Undefined Input Point 6	Not Assigned
7	Undefined Input Point 7	Not Assigned
8	Undefined Input Point 8	Not Assigned
9	Undefined Input Point 9	Not Assigned
10	Undefined Input Point 10	Not Assigned
11	Undefined Input Point 11	Not Assigned
12	Undefined Input Point 12	Not Assigned
13	Undefined Input Point 13	Not Assigned
14	Undefined Input Point 14	Not Assigned
15	Undefined Input Point 15	Not Assigned
16	Undefined Input Point 16	Not Assigned
17	Undefined Input Point 17	Not Assigned
18	Undefined Input Point 18	Not Assigned
19	Undefined Input Point 19	Not Assigned
20	Undefined Input Point 20	Not Assigned
21	Undefined Input Point 21	Not Assigned
22	Undefined Input Point 22	Not Assigned

2. Click on the *Input #, Description* or *Zone* text to proceed. A screen as shown below appears.



3. Delete the default text in the *Description* field and enter the new *Description*.
4. Delete the default entry for *Arm Delay* and enter the new Arm Delay (this field is a hyperlink to the first Input Point if this is the second or subsequent Input Point of an Alarm Zone). If you want immediate Arming/Disarming, leave it as 0. Value from 1 to 255 will cause a delay before the Alarm Zone is armed. During this delay any triggering of the Input Points will not be considered as an Alarm.
5. Delete the default entry for *Alarm Delay* and enter the new Alarm Delay (this field is a hyperlink to the first Input Point if this is the second or subsequent Input Point of an Alarm Zone). If you want the Alarm to be activated immediately when the Input Point is triggered during Arm condition, leave it as 0. Value from 1 to 255 will cause a delay before Alarm activation. During this delay period, if the Input Point restored to normal or user Disarm the Alarm Zone, no alarm will be activated. Alarm activation will cause the Output Relay configured in the *Alarm Status* to turn on.

NOTICE!

The *Alarm status* Output Relay assigned here is the same one that is listed at the *Output Setup*. By setting the *Duration* to a value other than 0 at the *Output Setup* will cause the *Alarm* status Output Relay to turn on for the configured duration only. Leaving it as 0 will cause the Output Relay to remain on till the Alarm Zone is disarmed or the Input Point has restored to normal condition. Please refer to the section on *Output Setup* below for more details.

6. Select the Alarm Zone to which this Input Point is to group with, from the list. If you do not wish to assign it to Alarm Zone, just *select Not Assigned.* However, it must at least be assigned to a Schedule for this configuration to function.
7. Select the Schedule from the list. If you do not wish to assign it to a Schedule, just leave it as *Undefined*. However, it must at least be assigned to an Alarm Zone for this configuration to function. (This field is disabled if this is the second or subsequent Input Point of an Alarm Zone).
8. Select the appropriate Output Point, for the various Status Outputs, from the list. By default, these Outputs are *Not Assigned*.

NOTICE!
The Output Points listed/assigned here are the same as those listed at the *Output Setup*. By setting the Duration to a value other than 0 at the *Output Setup* will cause the Status Output Relays to turn on for the configured duration. Leaving it as 0 will cause the Output Relays to remain on till the Status has changed. Please refer to the section on *Output Setup* below for more details.

9. Click on the button (see NOTICE1, 2, and 3).

NOTICE!

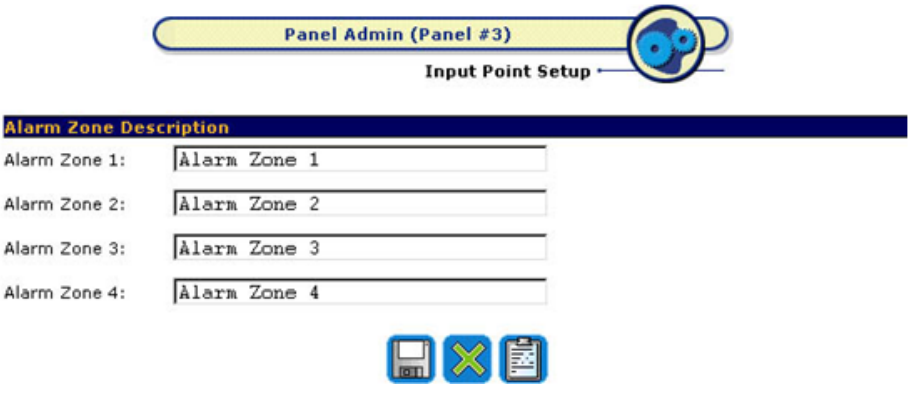
1. Activating the button will cause all active (Armed) Input Points within the Alarm Zone to be set to default, i.e. Disarmed.
2. Activating the button outside the pre-defined Schedule intervals will cause the Input Point to be Armed.
3. When an Alarm Zone is also armed/disarmed by Schedule, the condition similar to NOTICE 2 has the priority over NOTICE 1.

Proceed to configure other Input Points by clicking on the button to return to main page.

16.4.1 Alarm Zone Description

The *Alarm Zone Description* allows the user to change the description for each Alarm Zone to the description he prefers so that he may better visualize the location of the alarm zone.

From the first web page of the *Input Setup*, click on the Alarm Zone Description link. A screen as shown below appears.



1. To change the *Alarm Zone Description* for each Alarm Zone, delete the default description from each *Alarm Zone* and enter the new description accordingly.

16.4.2 How to generate a Print Preview of the Input Point Report

Once you have completed configuring the Input Points, a hardcopy can be printed out.

1. From the first web page of the Input Setup, click on the Input Point Report link. A screen as shown below appears.

Input #	Description	Zone
1	Motion Detector 1	Alarm Zone 1
2	Motion Detector 2	Alarm Zone 1
3	Motion Detector 3	Alarm Zone 2
4	Motion Detector 4	Alarm Zone 2
5	Motion Detector 5	Not Assigned
6	Undefined Input Point 6	Not Assigned
7	Undefined Input Point 7	Not Assigned
8	Undefined Input Point 8	Not Assigned
9	Undefined Input Point 9	Not Assigned
10	Undefined Input Point 10	Not Assigned
11	Undefined Input Point 11	Not Assigned
12	Undefined Input Point 12	Not Assigned
13	Undefined Input Point 13	Not Assigned
14	Undefined Input Point 14	Not Assigned
15	Undefined Input Point 15	Not Assigned
16	Undefined Input Point 16	Not Assigned
17	Undefined Input Point 17	Not Assigned
18	Undefined Input Point 18	Not Assigned
19	Undefined Input Point 19	Not Assigned
20	Undefined Input Point 20	Not Assigned
21	Undefined Input Point 21	Not Assigned
22	Undefined Input Point 22	Not Assigned

2. Select the desired Input Point from the *Input Description* list. If all Input Points are required, select *All Input Points*.

3. Click on the button for a print preview of the report. The following screen-capture shows a sample of the report.

Return To Input Point Setup Return To Selection Criteria

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

Input Point Report
Monday, 30 Aug 2004 16:24:41

Input # : 1
Description : Motion Detector 1
Arm Delay : 3 seconds
Alarm Delay : 3 seconds
Zone : Alarm Zone 1

Input Arm/Disarm Control
Arm/ Disarm : Criteria 1 (Toggle)

Output Link
Alarm Status : Motion Detector 1 (Simulator)
Arm/ Disarm Status : Not Assigned
Ready Status : Not Assigned
Bypass Status : Not Assigned

If you wish to print out a hardcopy, click on the Print button located on the Toolbar of the web browser program. Alternatively, click on the *File* and select *Print*.

4. To return to the Input Setup web page, click on the Return To Input Point Setup link.
5. To generate a preview of other input points, click on the Return To Selection Criteria link.

16.5 Output Setup

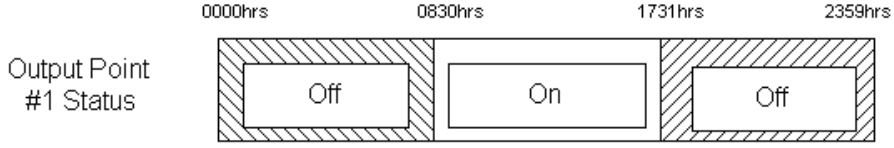
The Access Easy Controller has 32 user programmable Output Points that will be used for Utility Triggering purposes. The addresses for these Input Points range from 33 to 64 and are available on the I/O Card. Each card can provide up to 8 Output Points

The Output Points are triggered manually by user via the web page, or based on Schedule Intervals, or be triggered by an Input Point as a Status indicator. Please refer to section on Input Setup for detail.

The status of all the Output Points is displayed in the Output Control web page except those points that are triggered by Input Points. Please refer to the Chapter on Output Control for detail.

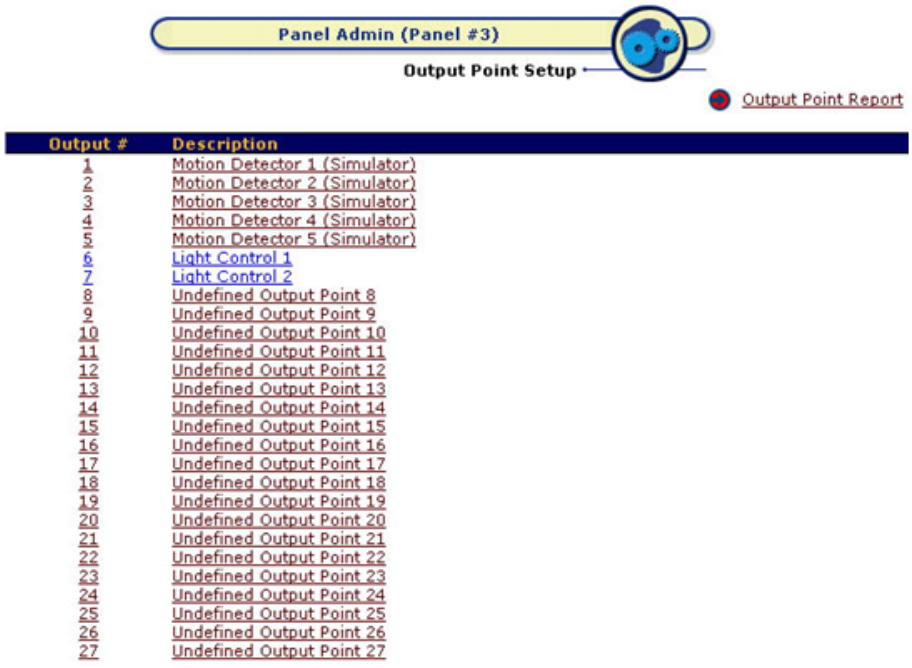
Before we start, here is a brief description of how the Access Easy Controller interprets the Schedule Intervals for Output Points triggering status.

For example,
If the setting for Schedule #2 is: -
Interval 1 Start 0830hrs End 1730hrs
Interval 2, 3, and 4 has no setting.
When the Schedule #2 is tied to Output Point #1, the point will turn on and off accordingly.

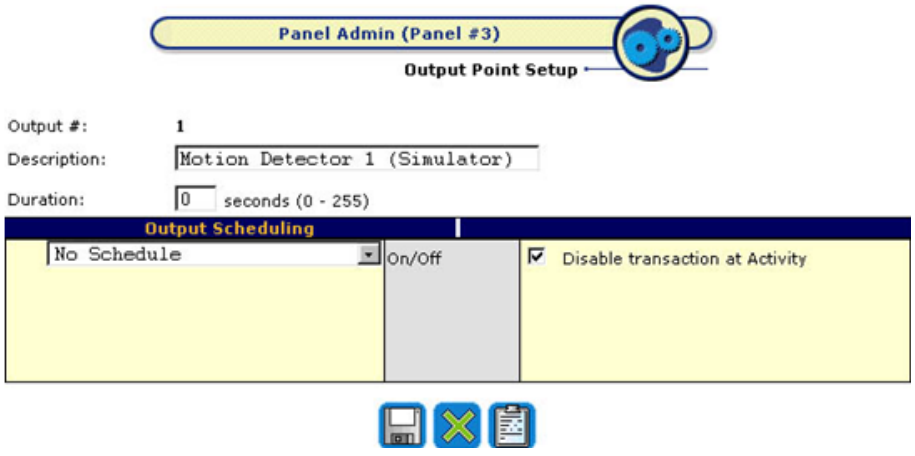


Take note that the Output Point switches On at exactly 0830hrs but switches Off at 1731hrs, a minute delay, as compared to the Schedule #2 setting. The reason is that Access Easy Controller takes 17:30:59hrs as a valid End time for 1730hrs.

To Setup the *Output Point* select the target Access Easy Controller


Panel Admin (Panel #3)
Output Point Setup
Output Point Report
Output # Description
1 Motion Detector 1 (Simulator)
2 Motion Detector 2 (Simulator)
3 Motion Detector 3 (Simulator)
4 Motion Detector 4 (Simulator)
5 Motion Detector 5 (Simulator)
6 Light Control 1
7 Light Control 2
8 Undefined Output Point 8
9 Undefined Output Point 9
10 Undefined Output Point 10
11 Undefined Output Point 11
12 Undefined Output Point 12
13 Undefined Output Point 13
14 Undefined Output Point 14
15 Undefined Output Point 15
16 Undefined Output Point 16
17 Undefined Output Point 17
18 Undefined Output Point 18
19 Undefined Output Point 19
20 Undefined Output Point 20
21 Undefined Output Point 21
22 Undefined Output Point 22
23 Undefined Output Point 23
24 Undefined Output Point 24
25 Undefined Output Point 25
26 Undefined Output Point 26
27 Undefined Output Point 27

1. Click on the *Output #* or *Description* text to proceed. A screen as shown below appears.



2. Delete the default text in the *Description* field and enter the new *Description*.
3. Delete the default entry for Duration and enter the new Duration (see NOTICE below).
4. By checking the box *Disable transaction at Activity*, user can disable any of the 32 output points activity, especially when they are activated by other type of function or elevator operation which don't require any logging.

NOTICE!

This setting for the *Duration* field is applicable for Manual Output Control (refer to *Output Control*). User can force the Output Point(s) to toggle its current state for the duration specified here. User could also assign the Output Point as a Status Output for the Input Point. However, if the *Duration field* has a value other than 0, the Output Point will not remain on when the respective status is activated. Instead, it will turn on only for the duration as specified here.

5. Select the appropriate Schedule from the list. By default, an unused Output Point is tied to *No Schedule* i.e. the Output will not be triggered.

6. Click on the button.

NOTICE!

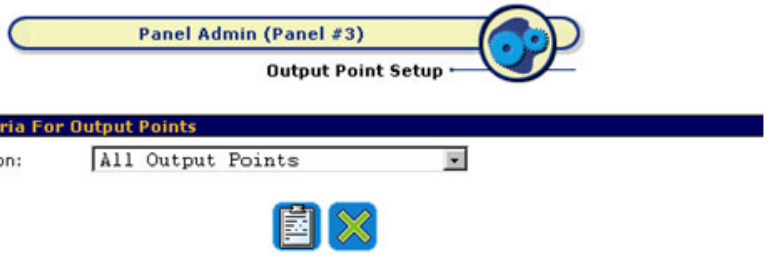
Activating the button within the pre-defined Schedule intervals will cause the Output Relay to turn On.

7. Click on the button to return to main page.

16.5.1 How to Generate a Print Preview of the Output Point Report

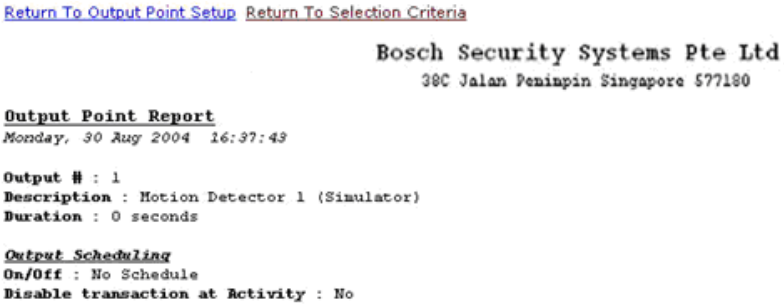
Once you have completed configuring the Output Points, a hardcopy can be printed out.

1. From the first web page of the Output Setup, click on the Output Point Report link. A screen as shown below appears.



2. Select the desired Output Point from the *Output Description* list. If all Output Points are required, select *All Output Points*.

3. Click on the button for a print preview of the report. The following screen-capture shows an example of the report.


Return To Output Point Setup
Return To Selection Criteria
Bosch Security Systems Pte Ltd
38C Jalan Peminpin Singapore 577180
Output Point Report
Monday, 30 Aug 2004 16:37:43
Output # : 1
Description : Motion Detector 1 (Simulator)
Duration : 0 seconds
Output Scheduling
On/Off : No Schedule
Disable transaction at Activity : No

4. To return to the Output Setup web page, click on the Return To Output Point Setup link.

5. To generate a preview of other output points, click on the Return To Selection Criteria link.

16.6 Advance I/O Setup

The basic need for such an operation is to enable the rerouting of physical or logical information from one operation to another. Due to its flexibility, the type of operation it can achieve is dependent on the installer. Besides normal input, output and schedule selection, some functions will allow:-

- Inter-connection with other functions.
- Criteria to select 'Where', 'What' and 'Who' (individual and access group) as well as Key input.
- Always 'On' or 'Off'.

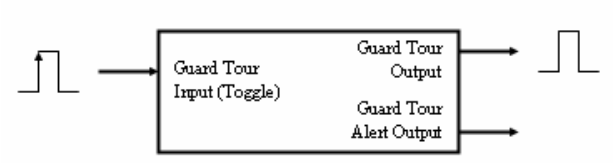
Some of the advance functions that it can support are:-

- Guard Tour
- Feed Through
- OR Logic
- AND Logic
- XOR Logic
- NAND Logic
- Interlock / Man Trap
- Up-Down Counter
- Exit Door
- One Shot

A description of each item will be given below.

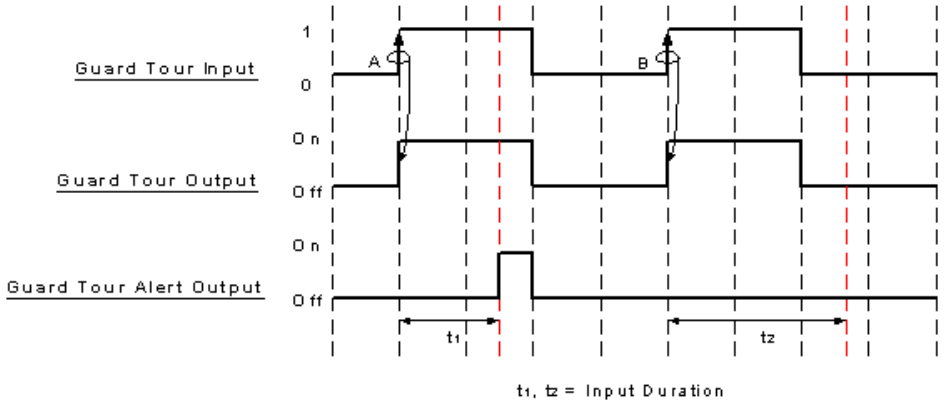
16.6.1 Guard Tour

This function is used when the block is used as one of the guard tour stations in the guard tour routes.A toggle key switch can be used to activate guard tour registration. If key is switched to ON state and is not removed, a reminder alarm will be activated.



Input/Output	Description
Guard Tour Input	This input is edge triggered from '0' to '1' (leading edge) & toggling. A key switch can be connected to this input.
Guard Tour Ouput	A LED is normally connected to this output. The LED will be turned on for the duration when the guard tour input is triggered.
Guard Tour Alert Ouput	A LED is normally connected to this output. The LED will be turned on when the Input Duration has lapsed and the key switch, which is switched to ON state, is still not removed. A reminder alarm will be activated.

The timing diagram below gives a graphical description of the function.



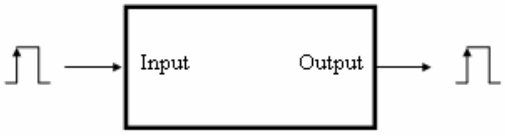
In the timing diagram above, Guard Tour Input at transition A and B will cause the Guard Tour Output to be turned On for the duration when the Guard Tour Input is triggered. When the Input Duration, t1, has lapsed and the Guard Tour Input is still at High (1), the Guard Tour Alert Output will be turned On until the Guard Tour Input is switched to Low (0). Whereas for t2, the Input Duration is such that the Guard Tour Input has already been switched to Low (0) before the Input Duration, t2, has lapsed. Therefore the Guard Tour Alert Output is not triggered.

In practical scenario, a key switch is normally connected to the Guard Tour Input, a LED connected to Guard Tour Output and a LED and/or an alarm is connected to the Guard Tour Alert Output. When the guard goes for his daily routine, he would turn his key switch to On state. This will cause the LED in the Guard Tour Output to be turned On. And if the key is not removed after the Input Duration has lapsed, the LED in the Guard Tour Alert Output will be turned On and the alarm will be activated to remind the guard that he has not removed the key from the key switch.

16.6.2 Feed Through

This function is used when the output of a function block has to be fed into the input of another function block for further action.

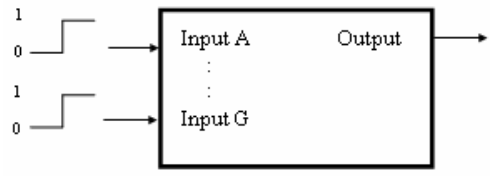
This function will enable any type of output such as physical output, link or reader control to follow the input such as physical input, physical output, link, criteria or schedule. Each item is explained in the above section Input Point Able to Arm/Disarm by Other Type of Input. Level or toggle input behavior can be selected.



Input/Output	Description
Input source	The input will be linked to the output directly. It is edge triggered from '0' to '1' (leading edge) & toggling.
Output	The output is a direct link of the input.

16.6.3 OR Logic

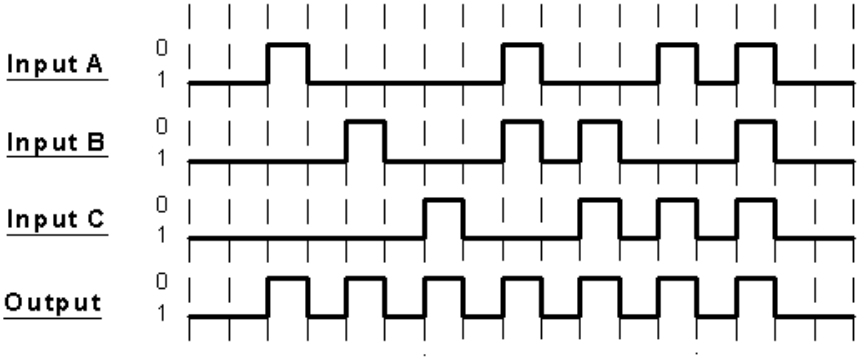
This function is used in cases whereby the output of a function block is to be triggered when any one or more of the stated conditions is fulfilled. In Advance I/O Setup, a maximum of 7 conditions is allowed.



The output is set to high when one or more of the stated inputs is set to high. The following table depicts the OR logic operation, assuming only 3 inputs are used.

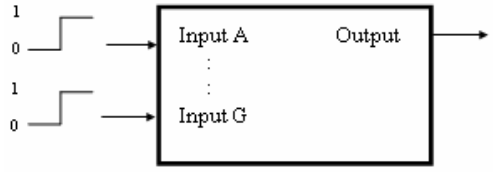
Input A	Input B	Input C	Output
0	0	0	0
1	0	0	1
0	1	0	1
0	0	1	1
1	1	0	1
0	1	1	1
1	0	1	1
1	1	1	1

The timing diagram below gives a graphical description of the function.



16.6.4 AND Logic

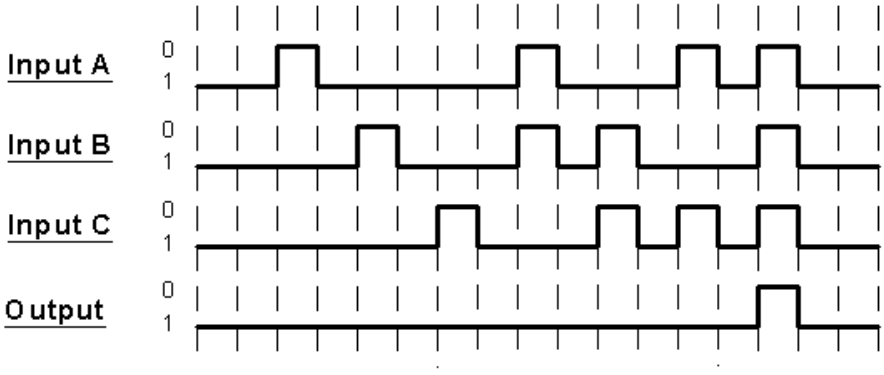
This function is used in cases whereby the output of a function block is to be triggered when all the stated conditions are fulfilled. In Advance I/O Setup, a maximum of 7 conditions is allowed.



The output is set to high when all of the stated inputs are set to high. The following table depicts the AND logic operation, assuming only 3 inputs are used.

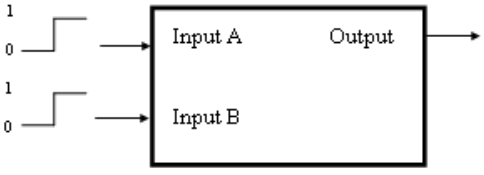
Input A	Input B	Input C	Output
0	0	0	0
1	0	0	0
0	1	0	0
0	0	1	0
1	1	0	0
0	1	1	0
1	0	1	0
1	1	1	1

The timing diagram below gives a graphical description of the function.



16.6.5 XOR Logic

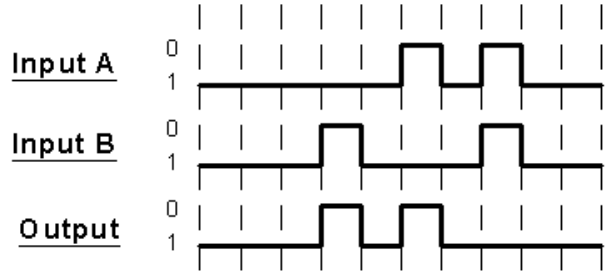
This function is used in cases whereby the output of a function block is to be triggered when all the stated conditions are different. In Advance I/O Setup, a maximum of 7 conditions is allowed.



The output is set to high when all the stated inputs are at different states. The following table depicts the XOR logic operation, assuming only 2 inputs are used.

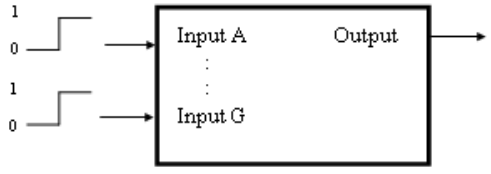
Input A	Input B	Output
0	0	0
0	1	1
1	0	1
1	1	0

The timing diagram below gives a graphical description of the function.



16.6.6 NAND Logic

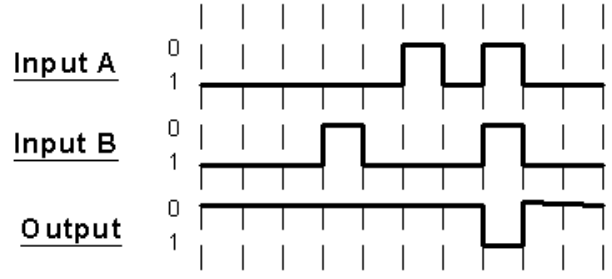
This function is used in cases whereby the output of a function block is to be triggered when one or more of the input states is low.



The output is set to high when one or more of the input states is low. The following table depicts the NAND logic operation, assuming only 2 inputs are used.

Input A	Input B	Output
0	0	1
0	1	1
1	0	1
1	1	0

The timing diagram below gives a graphical description of the function.



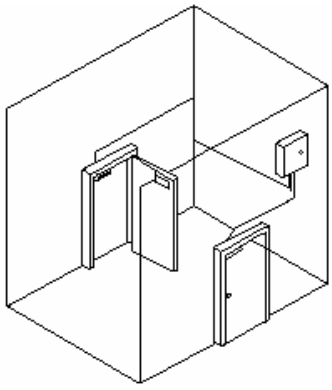
16.6.7 Interlock / Man Trap

1. Interlock Operation

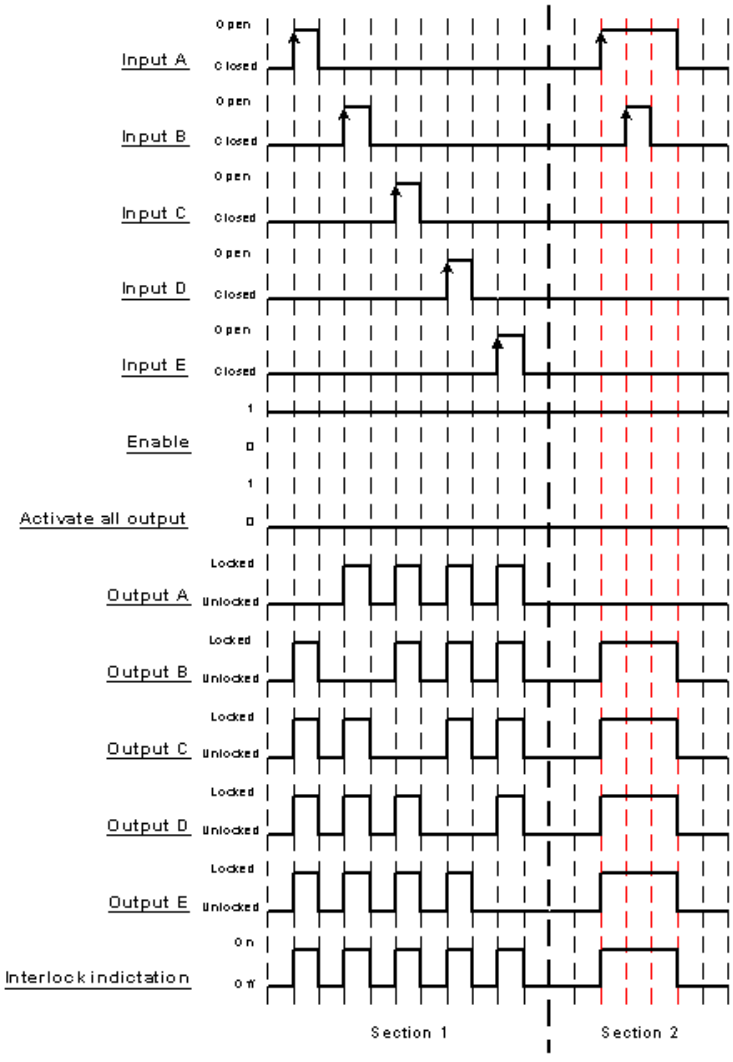
All doors will remain closed and unlocked. Opening any of the doors will cause all other doors to be locked until the opened door returns to the closed position. In Access easy controller, a maximum of 5 doors is configurable.

Examples of such applications are darkrooms, laboratories, clean rooms, airlock rooms, X-ray or other treatment rooms.

The figure below shows an illustration of Interlock Operation for 2 doors.



The timing diagram below gives a graphical description of the function.


Input A
Open
Closed
Input B
Open
Closed
Input C
Open
Closed
Input D
Open
Closed
Input E
Open
Closed
Enable
1
0
Activate all output
1
0
Output A
Locked
Unlocked
Output B
Locked
Unlocked
Output C
Locked
Unlocked
Output D
Locked
Unlocked
Output E
Locked
Unlocked
Interlock indictation
On
Off
Section 1
Section 2

Section 1

In Section 1, a leading edge from '0' to '1' is detected at Input A first. This means that the door at A is opened. This causes the door at A to be unlocked (Output A-Low) and the rest of the doors to be locked (Output-High) until door at A is closed. The same applies when each door is opened in turn.

Enable is always high (In Access easy controller configuration, Enable can be configured as "Always On"). *Activate all output* is always low (In Access easy controller configuration, *Activate all output* can be configured as "Always Off").

Section 2

In Section 2, a leading edge from '0' to '1' is first detected at Input A. From Section 1, we know that the door at A is opened and this causes the door at A to be unlocked (Output A-Low) and the rest of the doors to be locked (Output-High) until door at A is closed.

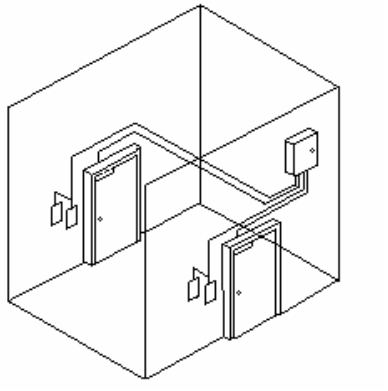
But before door at A is closed, someone tries to open door at B. He cannot open the door at B as it is locked (Output B-High) as door at A has not been closed back to original position.

2. Man Trap Operation

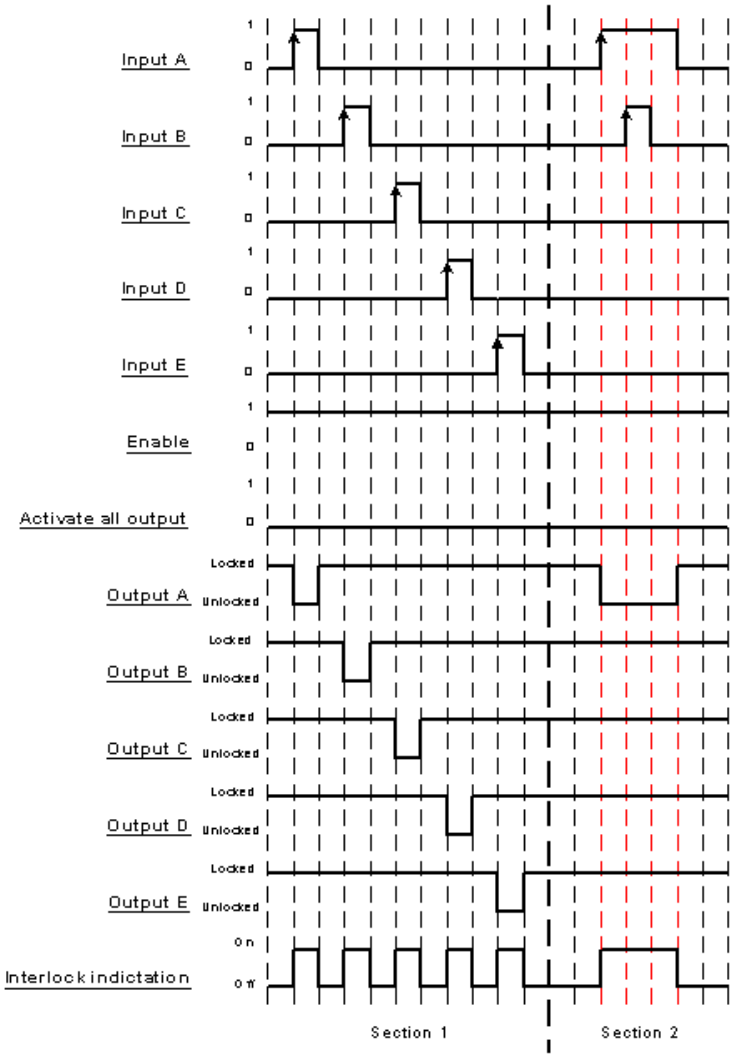
All doors are normally closed and locked. Unlocking any door by reader causes the other doors to be incapable of being unlocked. In Access easy controller, a maximum of 5 doors is configurable.

Examples of such applications are restricted darkrooms, laboratories, clean rooms, airlocks, showers, money counting rooms and computer rooms.

The figure below shows an illustration of Mantrap for 2 doors.



The timing diagram below gives a graphical description of the function.



Section 1

In Section 1, a leading edge from '0' to '1' is first detected at Input A, i.e someone presents his card at reader for door A. This means that door A will be unlocked (Output A-Low) and the rest of the doors will be incapable of being unlocked (Output-High). The same applies when card is presented to the readers at the other doors in turn.

Enable is always high (In Access easy controller configuration, Enable can be configured as "Always On"). A*ctivate all output* is always low (In Access easy controller configuration, *Activate all output* can be configured as "Always Off").

Section 2

In Section 2, a leading edge from '0' to '1' is first detected at Input A. From Section 1, we know that when someone presents his card at reader for door A, door A will be unlocked (Output A-Low) and the rest of the doors to be incapable of being unlocked (Output-High).

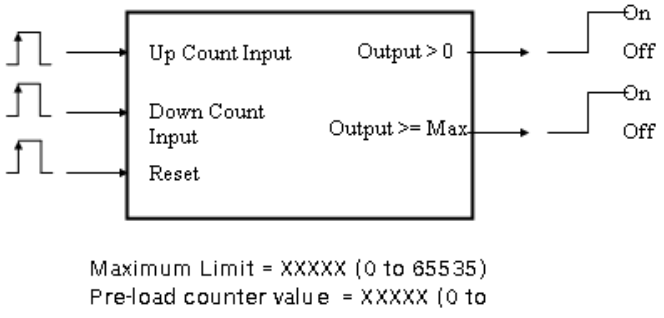
But before door A is locked back, someone presents his card at door B. He cannot unlock door B as it is incapable of being unlocked (Output B-High).

Both the above operations, Interlock Operation and Mantrap can be easily configured by monitoring the door strike and contact status.

The number of doors that can be configured for these operations is only limited by the number of I/O and Reader available per controller

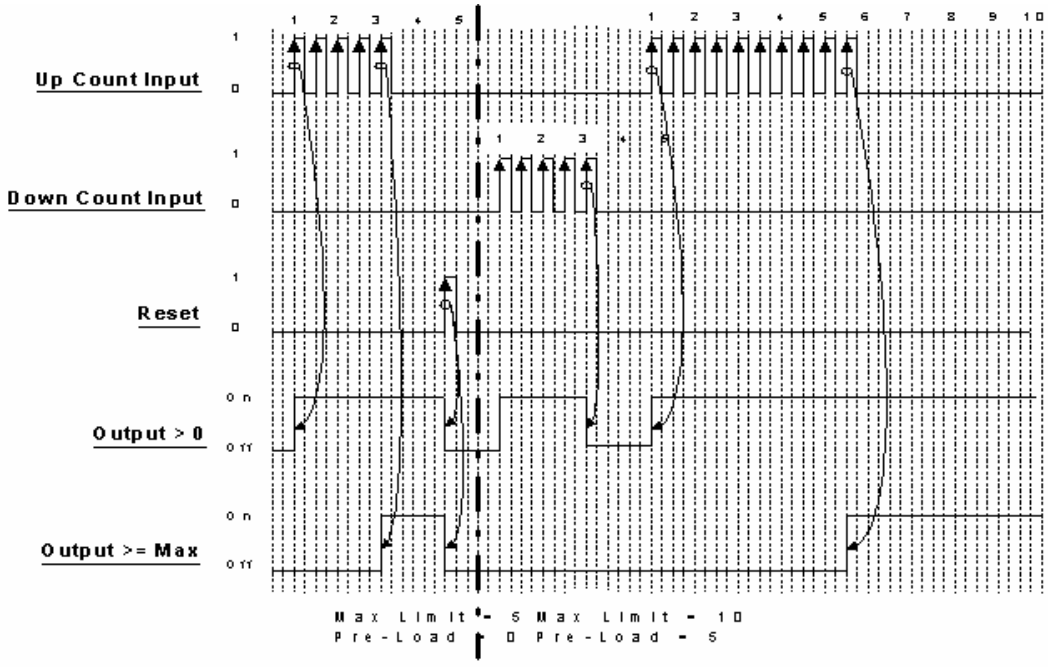
16.6.8 Up-Down Counter

This function enables the tracking of the number of card holder/event and is able to trigger output or control based on the maximum configuration limit.



Input/Output	Description
Up count Input	Increment the counter when a low to high edge is detected.
Down count Input	Decrement the counter when a low to high edge is detected.
Reset	Reset the counter to zero when a low to high edge is detected.
Output > 0	Set high when the counter is not zero, and set low when the counter is zero.
Output >= Max	Set high when the counter is greater than or equal to the maximum limit, else set low.

The timing diagram below gives a graphical description of the function.



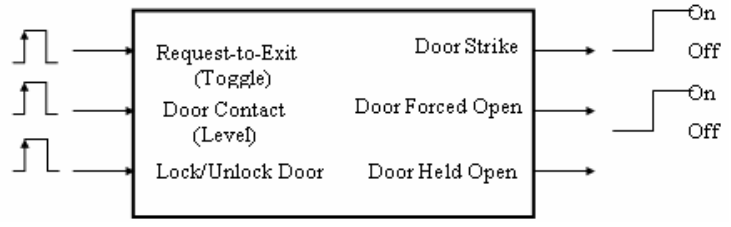
In the timing diagram, the basic operation of the function is outlined below: -

Max Limit = 5 and Pre-Load = 0
With the 2 defined parameters, the Output>=Max will be driven high on the 5th pulse on the Up Count input. However, the Output>0 is driven high on the first pulse. A Reset pulse clears both outputs to zero.

Max Limit = 10 and Pre-Load = 5
With a Pre-Load of 5 count, the Output>0 is driven high. This Output>0 will be cleared on the 5th pulse on the Down Count input.
A pulse on the Up Count input drives the Output>0 high again and the Output>=Max will be driven high on the 10th pulse.

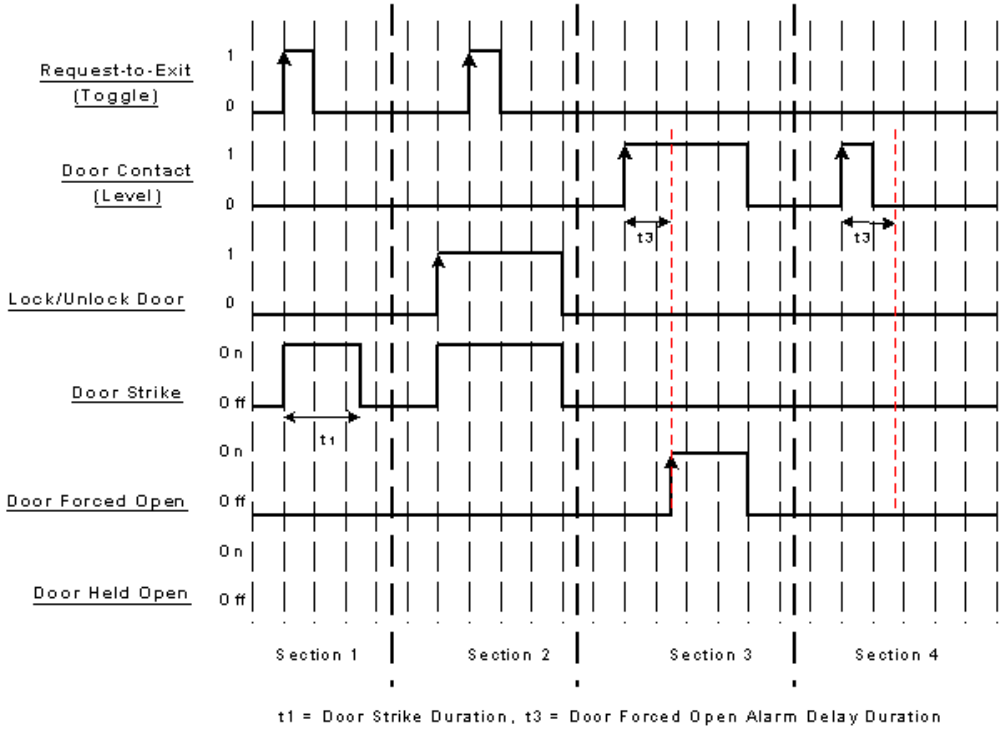
16.6.9 Exit Door

This function is mainly used to monitor and control emergency exit doors.



Input/Output	Description
Request-to-Exit (Toggle)	This input is edge triggered from '0' to '1' (leading edge) & toggling. It activates the Door Strike output for a period of the Door Strike Duration when a leading edge is detected.
Door Contact (Level)	This input is edge triggered from '0' to '1' (leading edge). It activates the Door Forced Open output when a leading edge is detected and a period of the Door Forced Open Alarm Delay Duration has passed.
Lock/Unlock Door	Permanently locks/unlocks the door when activated.
Door Strike	Driven to high for a period of Door Strike Duration when a leading edge is detected at Request-to-Exit.
Door Forced Open	Driven to high for the duration when Door Contact is high when a leading edge is detected at Door Contact and the Door Forced Open Alarm Delay Duration has lapsed.
Door Held Open	Driven to high when the Door Strike Duration is over and subsequently, the Door Open Duration is over.

The timing diagram below gives a graphical description of the function



In the timing diagram, it is divided into 4 sections. The basic operation of each section is outlined below: -

Section 1

In Section 1, a leading edge from '0' to '1' is detected at Request-to-Exit. This causes the Door strike to be driven high for a duration of t1, the Door Strike Duration.

Section 2

In Section 2, a leading edge is first detected at Lock/Unlock Door. This causes the Door strike to be driven high for the duration when the Lock/Unlock Door is triggered. Since the Door Strike is already at state high, meaning it is de-energised, when a leading edge is detected at Request-to-Exit, there is no difference in Door Strike.

Section 3

In Section 3, a leading edge is detected at Door Contact. However there is a Door Forced Open Alarm Delay Duration of period t3. Hence the Door Forced Open is driven high only after the Door Forced Open Alarm Delay Duration has passed and remains high until the Door Contact is triggered low. The Door Forced Open Alarm Delay Duration is to ensure that the alarm is genuine and not caused by noise or interference.

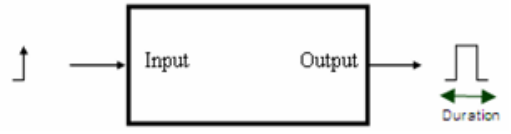
Section 4

In Section 4, a leading edge is detected at Door Contact. However the signal lasts for a period less than the Door Forced Open Alarm Delay Duration of period t3. Therefore the Door Forced Open output is not activated. This is because the signal detected could be due to noise or interference

16.6.10 One Shot

This function is similar to Feed Through except it is used when the output of a function block is triggered for a predefined duration when input state is high.

This function will enable any type of output such as physical output, link or reader control to follow the input such as physical input, physical output, link, criteria or schedule.



Input/Output	Description
Input source (Toggle)	The input will be linked to the output directly. It is edge triggered from '0' to '1' (leading edge).
Output	The output is a direct link of the input.

16.7 Input Point Configuration

The state of each Input point must be closed in order for the Access Easy Controller to treat it as normal state. However, there are some devices whereby its *normal state* is open thus, representing an activated / alarm state.

When such devices are connected to these Input points, without inverting an input's to the *normal state*, it would cause unexpected or false alarm.
In simple term, this configuration allows user to inverts the logical state of the input that is seen by the Access Easy Controller thus allowing such devices to be used.

Access Easy Controller allows all the Input Points to be inverted except those assigned to Exit Readers and Arm/Disarm Readers.

In this section, users can also select the Input Point to be in 2 State Non-Supervised, 2 State Supervised or 4 State Supervised monitoring state.

16.7.1 To activate Input Point Configuration

To configure the Input Point Configuration, select the target Access Easy Controller and click on the *Input Point Configuration* hyperlink. The following screen will appear.

Readers 1-8 Readers 9-16 Inputs 1-16 Inputs 17-32

Input Point Configuration

Inverted Input Points Clear All Select All Manual

Inverted Input #		Description	2 State Non Supervised	2 State Supervised	4 State Supervised
1	☐	Main Entrance - Request to Exit	◉	○	○
2	☐	Main Entrance - Door Contact	◉	○	○
3	☐	Side Entrance - Request to Exit	◉	○	○
4	☐	Side Entrance - Door Contact	◉	○	○
5	☐	R&D Dept Entry Reader - Request to Exit	◉	○	○
6	☐	R&D Dept Entry Reader - Door Contact	◉	○	○
7	☐	Production Dept Entry Reader - Request to Exit	◉	○	○
8	☐	Production Dept Entry Reader - Door Contact	◉	○	○
9	☐	Production Dept Exit Reader - Request to Exit	◉	○	○
10	☐	Production Dept Exit Reader - Door Contact	◉	○	○
11	☐	Project Dept Entry Reader - Request to Exit	◉	○	○
12	☐	Project Dept Entry Reader - Door Contact	◉	○	○
13	☐	Sales Dept Entry Reader - Request to Exit	◉	○	○
14	☐	Sales Dept Entry Reader - Door Contact	◉	○	○

NOTICE!
Input 9 and 10 are assigned to Reader #5 - Production Dept Exit Reader. Since Reader #5 is defined as an Exit Reader, the check boxes are disabled.

To select Input Point Configuration

Using Manual

This is the default selection.

1. To assign the required *Input Point Configuration* for the inversion, click on the corresponding *Input Point Configuration* check boxes to show a tick mark. To de-select the point, click on it again.

2. Click on the button. Alternatively, click on the button to select the next sets of Input Points. User can also select from the sets of inputs from the links at the top, such as Readers 1-8, Readers 9-16, Inputs 1-16 or Inputs 17-32.

Using Select All

This is very useful if the number of Input Points need to be selected is more than ¾ of what is displayed. You can use this function then de-select those unwanted Input Points.

NOTICE!

The Select All and the Clear All function will only select / clear the 16 Input Points seen on the current web page. For the other Input Points on the other pages, user will have to go to the page and select / clear.

1. To select all, click on the *Select All* radio button. To de-select, click on *Clear All* or *Manual* radio button.

2. Click on the to refresh the screen and the selection returns to default (Manual is selected). If not all the *Inverted Input Points* are required, proceed to de-select by clicking on its corresponding check boxes. However, if all Points are required, you can straight away click on the button to save. Alternatively, click on the button to go to next sets of Input Points. User can also select from the sets of inputs from the links at the top, such as Readers 1-8, Readers 9-16, Inputs 1-16 or Inputs 17-32.

Using Clear All

This function works in reverse of the *Select All* function. Please refer to the above procedure.

16.7.2 To Select 2 State Non-Supervised, 2 State Supervised or 4 State Supervised

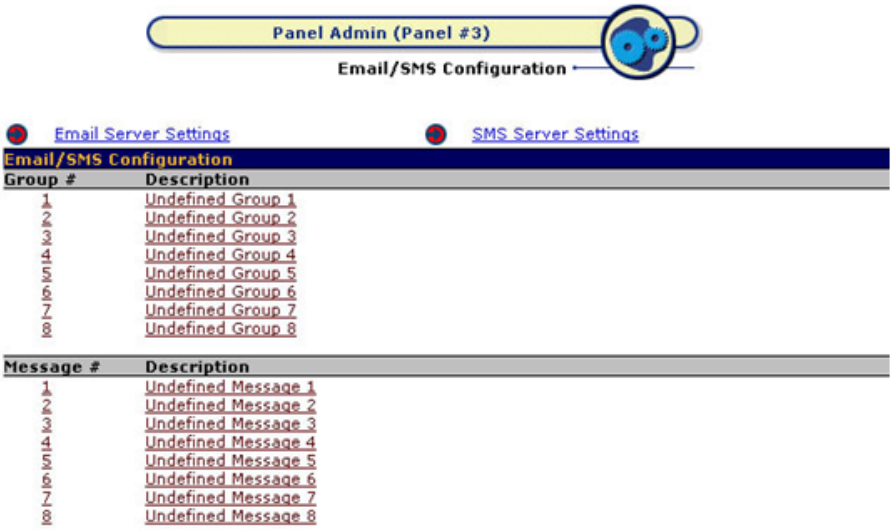
This will provide the system installer to have the flexibility of configuring any input in the panel to be in any monitoring requirement.

The panel will report fault in open or short condition only when the input is configured as 4 State Supervised monitoring.

1. To select either the 2 State Non-Supervised, 2 State Supervised or 4 State Supervised state, select the radio button belonging to the Input Point accordingly.

16.8 Email/SMS Configuration

To configure the Email/SMS Configuration, select the target Access Easy Controller and click on the *Email/SMS Configuration* hyperlink. The following screen will appear.



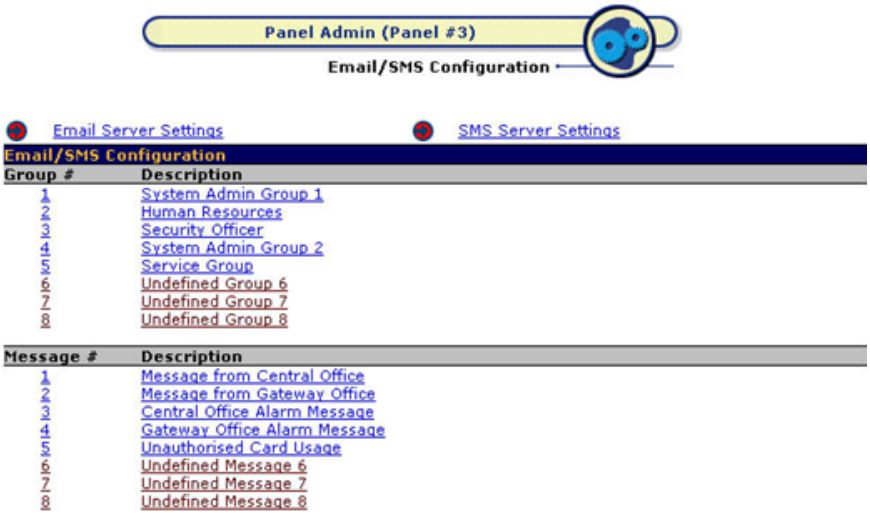
This function allows user to configure the Access Easy Controller to send out messages or Lateness Report using Simple Mail Transfer Protocol (SMTP) to email addresses. A total of eight groups and eight messages field are available for configuration. Each group has three "Send To" and three "Carbon Copy (Cc)" email addresses.

In order for the feature to work, user has to configure the various items, Devices, Cardholders, and Events in an AND operation. To exclude/disable an item(s) from the operation, the option Selected Only or Omit Only should be used with nothing selected. While for the Lateness Report, the feature is disable if no selection is made on any of the day of week (DOW).

A sample configuration for Lateness Report is presented at the end of the section.

To activate the Email/SMS Configuration:

1. From the Left Pane, click on the *Email/SMS Configuration* link. The screen as shown below appears.



2. Click on any of the *Group #* or its *Description* and you will be shown the Send To page.

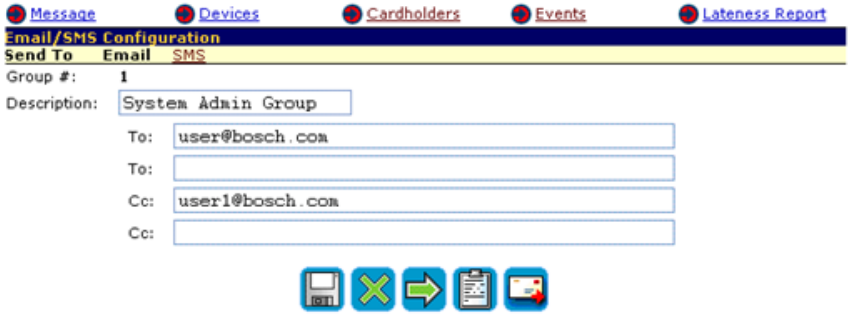
16.8.1 Send To

This web page allows user to configure the email addresses of the recipients. Up to two To and two Cc email addresses per group are available. The Access Easy Controller will ignore any configurations made for the group if there is no email address in any of the To fields even though there is email address in the Cc field. Each To and Cc should only contains one email address, entering more than one email address separating by a coma (,) or semi-coma (;) will be taken as a single email address, hence, not able to send out the mail to the recipients.

Send To Configuration (Email)

To edit the Send To Configuration for Email:

1. Click on the *Group #* or the *Description* text to proceed.

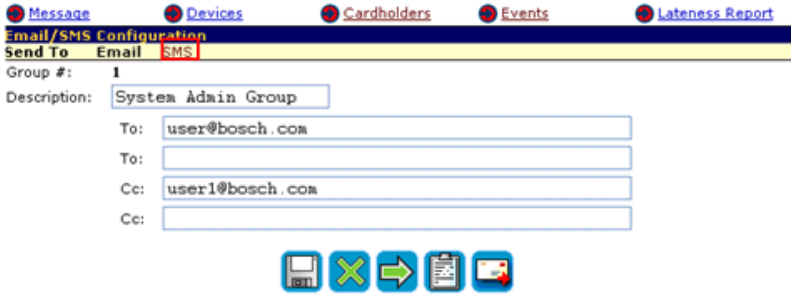


2. Click on the *SMS* hyperlink. The screen as shown below appears.
3. Highlight the default text and enter a Description for the Group.
4. Enter the email address in the appropriate field.
5. Click on the button.

Send To Configuration (SMS)

To edit the Send To Configuration (SMS):

1. Click on the *Group #* or the *Description* text to proceed.



2. From the screen above, click on the *SMS* link to configure the Send To Configuration for SMS. The screen as shown below appears.

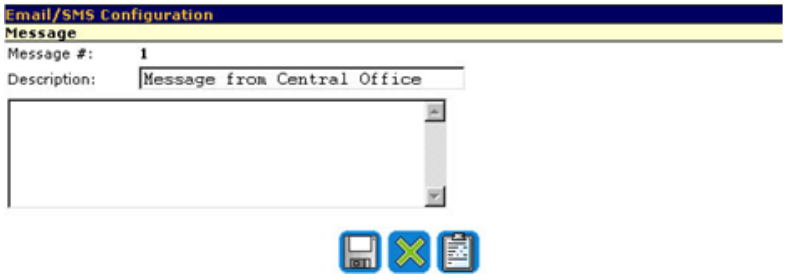
3. Enter the mobile numbers in the appropriate field.
4. Click on the button.

16.8.2 Message field

The Message field makes up the 'body text' while the Event is to appear in the 'subject' field of the dispatched email.

To edit the Message field:

1. Click on the *Message #* or the *Description* text to proceed.



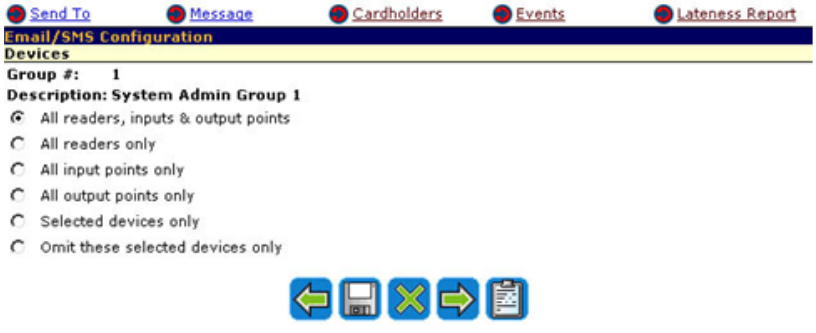
2. Highlight the default text and enter a Description for the Message.
3. Enter the new message limiting to 127 characters including punctuation.
4. Click on the button.
5. Click on the button to return.

16.8.3 Devices

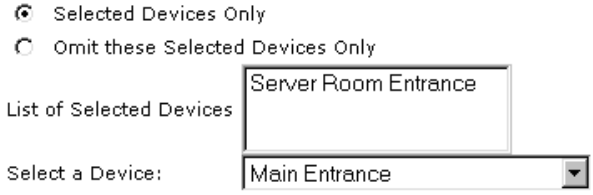
This web page allows user to configure the first (Devices) of the three items for the AND operation.

To edit the Email Configuration (Devices):

1. Click on the *Device* link or the button from the Sent To web page.



2. Select the desired radio button and click on the button.
If selection is made on either Selected Devices Only or Omit these Selected Devices Only, a window and a pull-down list appears as shown in the following diagram.



3. Select a device from the pull-down list and click on the button.
The selected device appears in the List of Selected Devices window. Repeat step 3 if you have other Devices to put on the list.

4. To delete selected device(s), click on the device name in the window followed by the button. Repeat step 4 if necessary.

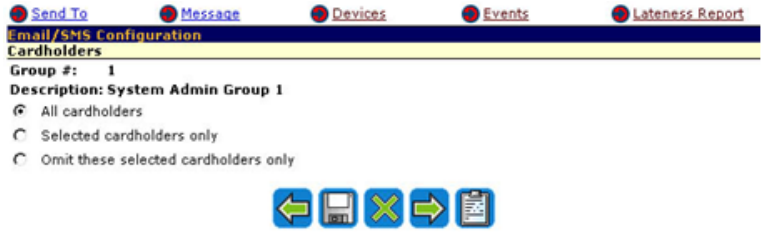
5. When you finish with your selection, click on the button.

16.8.4 Cardholders

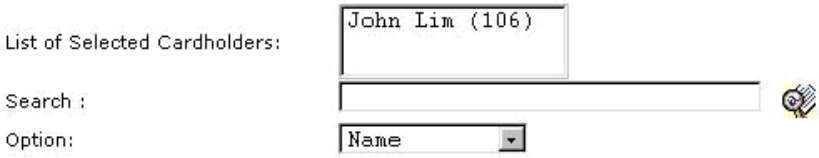
This web page allows user to configure the second (Cardholders) of the three items for the AND operation.

To edit the Email Configuration (Cardholders):

1. Click on the *Cardholders* link or the button from the Devices web page.



2. Select the desired radio button and click on the button.
If selection is made on either Selected Cardholders Only or Omit these Selected Cardholders Only, a window and the Search field appear as shown below. You have the option to search by Name, Card Number or the 2 User Field by selecting from the Option drop down box.



The function of Select By Card # and Select By Name is similar to the Search By Card # and Search By Name function respectively. Please refer to the explanation in *Chapter 6 Card Assignment*, How to Use Search Function for detail.

3. Select the Cardholder and click on the button.

The selected cardholder appears in the List of Selected Cardholders window. Repeat step 3 if you have other cardholders to put on the list (see NOTICE below).

NOTICE!
The List of Selected Cardholders window has a limit of up to 80 entries.

4. To delete selected Cardholder(s), click on the Cardholder's name in the window followed by the button. Repeat step 4 if necessary.

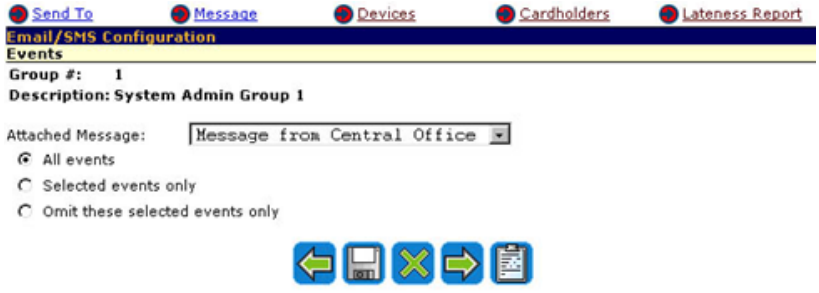
5. When you finish with your selection, click on the button.

16.8.5 Events

This web page allows user to configure the last (Events) of the three items for the AND operation.

To edit the Email Configuration (Events):

1. Click on the *Events* link or the button from the Cardholders web page.



2. Select the pre-defined Message from the list.

3. Select the desired radio button and click on the button.
If selection is made on either Selected Events Only or Omit these Selected Events Only, a window and a pull-down list appear as shown below.

4. Select the desired Event and click on the button.

The selected Event appears in the List of Selected Events window. Repeat step 4 if you have other Events to put on the list.

5. To delete selected Event(s), click on the Event in the window followed by the button. Repeat step 5 if necessary. When you finish your selection, click on the button.

User can refer to *Appendix D Email/SMS Configuration* Table for the combination of Devices, Cardholders and Events to select.

16.8.6 Lateness Report

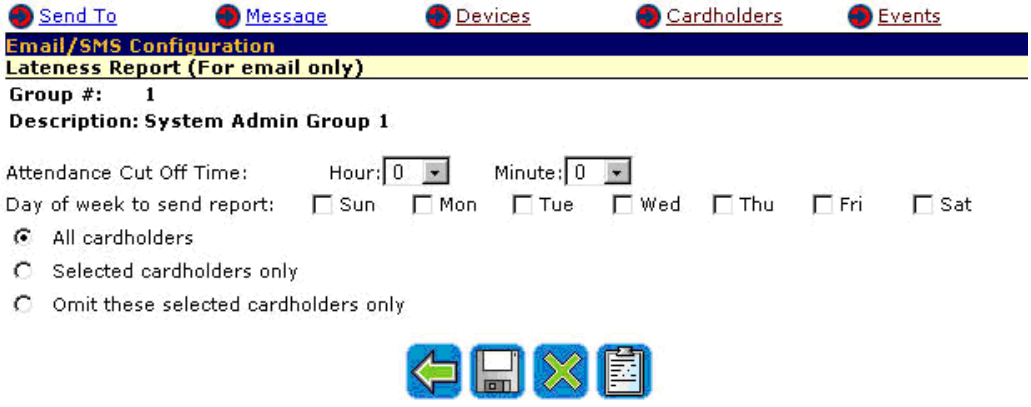
This web page allows user to configure the Lateness Report.

NOTICE!

The Lateness Report is to be used for keeping track of employee presence at the work place. It will consider an employee to be present for work once a transaction, bearing the employee's card number, is transacted. Card number(s) not transacted after the Attendance Cut off Time is regarded as late for work.

To edit the Email Configuration (Lateness Report):

1. Click on the *Lateness Report* link or the button from the Events web page.



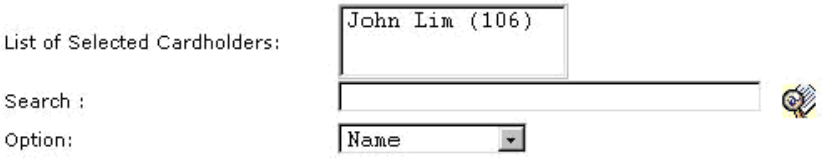
2. Select the Attendance Cut off Time Hour and Minutes from the list.

The *Attendance Cut off Time* defines the time on which the Panel checks through the current date's transactions for the presence of Card numbers and making comparison with respect to the Card database and the Selected/Omission list.

3. Select the appropriate Day of the week to send report check boxes.

The *Day of the week to send report* defines the day on which the Panel will keep track of the cut off time and to send out the report to the respectively email addresses.

4. Select the desired radio button and click on the button. If selection is made on either Selected Cardholders Only or Omit these Selected Cardholders Only, a window and the Search field appear as shown below. You have the option to search by Name or *Card Number* or *User Field* by selecting from the Option drop down box.



The function of Selection By Card # and Selection By Name is similar to the Search By Card # and Search By Name function respectively. Please refer to the explanation in the section on *Card Assignment, The Search Function* for detail.

5. Select the Cardholder and click on the button.The selected cardholder appears in the List of Selected Cardholders window. Repeat step 5 if you have other cardholders to put on the list.

NOTICE!
The List of Selected Cardholders window has a limit of up to 80 entries.

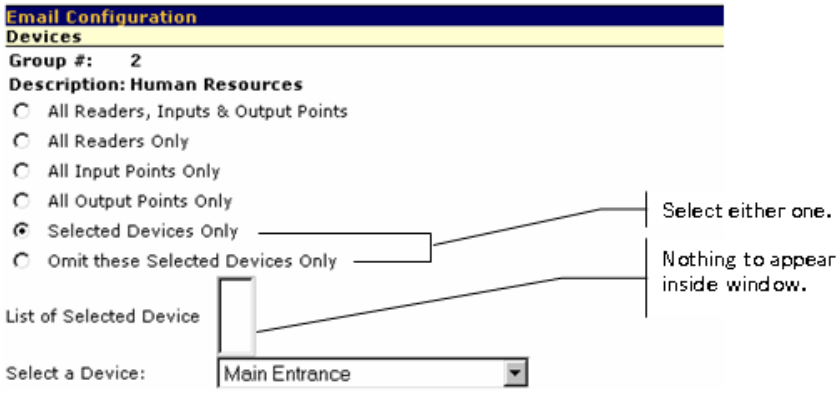
6. To delete selected Cardholder, click on the Cardholder's name in the window followed by the button. Repeat step 6 if necessary.

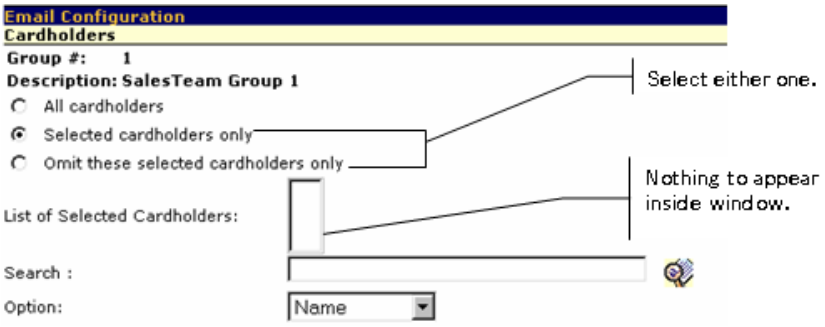
7. When you finish your selection click on the button.

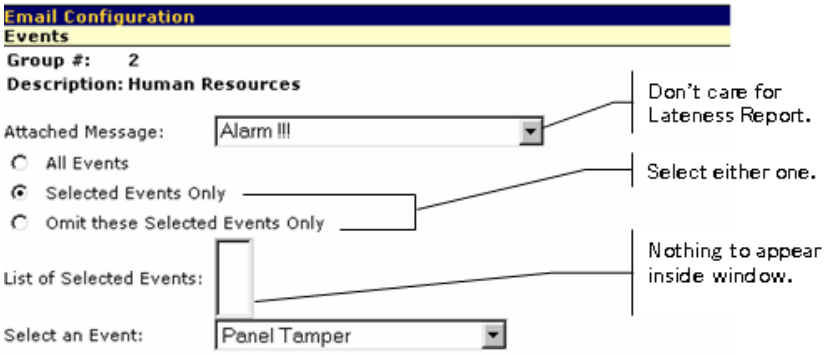
Sample Email Configuration for Lateness Report

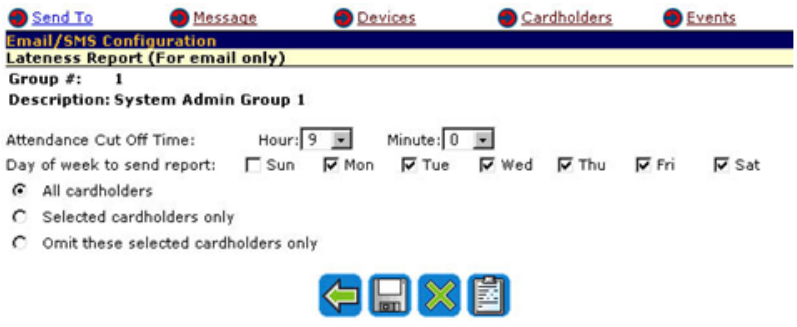
This section provides you with sample configuration for Lateness Report. The sample will instruct you on what to select for the four selection criteria (Devices, Cardholders, Events, and Lateness Report) in order to send out the email successfully. Please refer to the Appendix *"Email Configuration Table"* for more detailed configuration based on other Events.

For Lateness Report to be sent out, the items, Devices, Cardholders, and Events have to be disabled. That is, the Selected or Omit option is chosen but no specific parameter is selected. The following screen-capture shows the selection criteria for Devices, Cardholders, Events and Lateness Report respectively.


Email Configuration
Devices
Group #: 2
Description: Human Resources
All Readers, Inputs & Output Points
All Readers Only
All Input Points Only
All Output Points Only
Selected Devices Only
Omit these Selected Devices Only
List of Selected Device
Select a Device:
Main Entrance
Select either one.
Nothing to appear inside window.

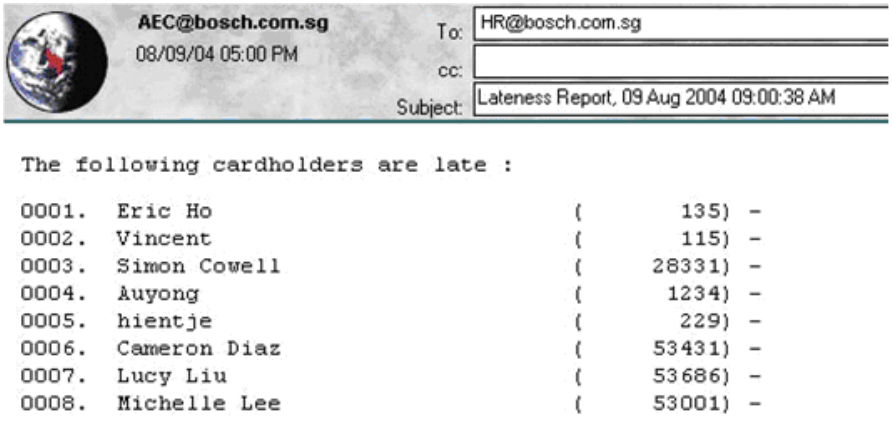

Email Configuration
Cardholders
Group #: 1
Description: SalesTeam Group 1
All cardholders
Selected cardholders only
Omit these selected cardholders only
List of Selected Cardholders:
Search :
Option:
Name
Select either one.
Nothing to appear inside window.


Email Configuration
Events
Group #: 2
Description: Human Resources
Attached Message:
Alarm !!!
All Events
Selected Events Only
Omit these Selected Events Only
List of Selected Events:
Select an Event:
Panel Tamper
Don't care for Lateness Report.
Select either one.
Nothing to appear inside window.

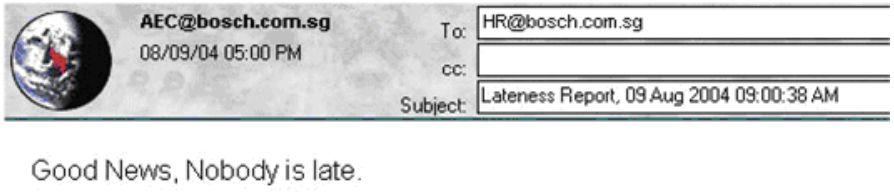

Send To
Message
Devices
Cardholders
Events
Email/SMS Configuration
Lateness Report (For email only)
Group #: 1
Description: System Admin Group 1
Attendance Cut Off Time:
Hour: 9
Minute: 0
Day of week to send report:
Sun
Mon
Tue
Wed
Thu
Fri
Sat
All cardholders
Selected cardholders only
Omit these selected cardholders only

With such configuration, the Panel will keep track of the cut-off time from Monday through Saturday (at 0900hrs) and will send out the Lateness Report to the recipient(s).
The screen-capture below illustrates what the email recipient(s) is expected to receive.

▶ The following Cardholders are late.


AEC@bosch.com.sg
08/09/04 05:00 PM
To: HR@bosch.com.sg
cc:
Subject: Lateness Report, 09 Aug 2004 09:00:38 AM
The following cardholders are late :
0001. Eric Ho (135) -
0002. Vincent (115) -
0003. Simon Cowell (28331) -
0004. Auyong (1234) -
0005. hientje (229) -
0006. Cameron Diaz (53431) -
0007. Lucy Liu (53686) -
0008. Michelle Lee (53001) -

▶ All Employees are punctual



16.8.7 Email Server Settings

This section allows user to define the address of the Outgoing Mail (SMTP) server, the SMTP port to use and the Access Easy Controller Email Address/Name. Click on the

Email Server Settings link to go to the Outgoing Mail (SMTP) server configuration page.

The Outgoing Mail (SMTP) Server defines the server that is to provide your email facilities and the Access Easy Controller's Email Address/Name is the reply address for emails sent by the Access Easy Controller; that is, the name address that is to appear in the 'sent to' field of the dispatched email.

Email Server Setup Information
Outgoing Mail (SMTP) Server: 129.2.0.86
Outgoing Mail (SMTP) Server Port: 25
WebCASt's Email Address/ Name: AEC@bosch.com.sg

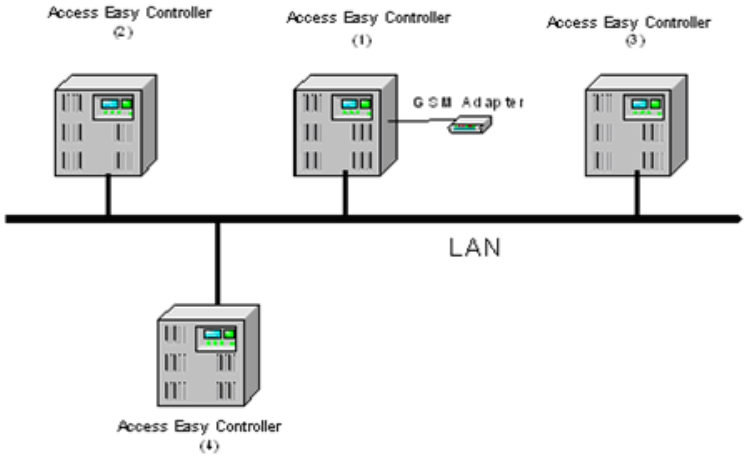
To edit the Email Server Setup Information

1. Highlight the default text in the Outgoing Mail (SMTP) Server field and enter the appropriate text.
2. The default number (25) is the commonly used port number for the Outgoing Mail (SMTP) Server, unless your configuration is different, we suggest you skip this field.
3. Enter the Access Easy Controller Address/Name as a complete word, with no spacing in between. You can use the underscore (_) to denote spacing. The Address/Name specified in this field will be used together with the Domain name to form the email address of the Access Easy Controller. Referring to the diagram and with the Domain name "bosch.com.sg", the email address of Access Easy Controller becomes, AEC@bosch.com.sg.
4. Click on the button.

16.8.8 SMS Server Settings

This section allows user to define the IP address of the Access Easy Controller that has a GSM adapter attached to its serial com acting as the SMS server. To briefly understood how the SMS feature works, we need to understand how the system should be configured.

The following diagram shows a drawing that has more than one Access Easy Controllers in the network. These panels work stand-alone but shared a common GSM adapter, which is attached to a dedicated Access Easy Controller serial com port.



The Access Easy Controller (1) has the GSM adapter connected to it's serial com port, hence, it is also acting as a SMS Server to help relay the other Access Easy Controllers' messages to the Service Provider.

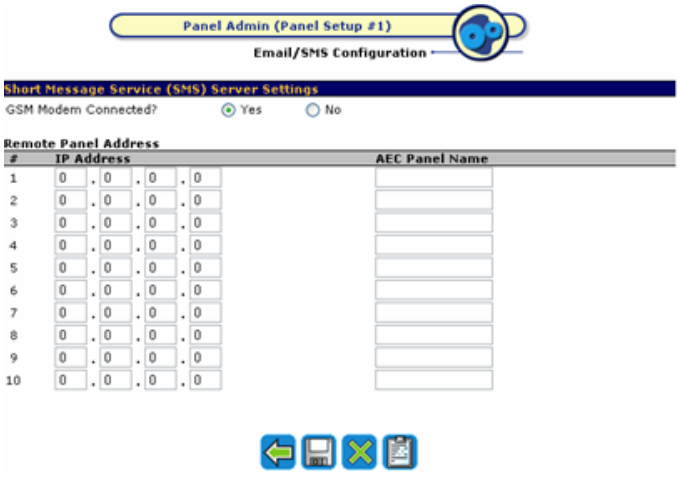
Whenever, there is any SMS message that needed to be send, the respective Access Easy Controller will send the SMS messages over to the Access Easy Controller SMS Server and the SMS Server will send via the GSM adapter to the Service Provider. These panels are said to be acting as the SMS Client. Hence, there is a need to control which is the IP Address that is allowed to send SMS, this is to prevent unauthorised personnel sending SMS via your Access Easy Controller.

NOTICE!
Please ensure that GSM adapter baudrate is configure at 115200bps, 8bit data, 1 stop bit and no parity settings. Please refer to the Appendix Gfor details.

To Configure Access Easy Controller as a SMS Server

By default, the SMS Server IP address is blank. If this panel is attached to a GSM adapter, you will need to configure the IP address of other Access Easy Controllers that will send SMS message through it.

1. To change this setting, click on the SMS Server Settings link. The screen as shown below appears.



2. By default, the radio button for *GSM Modem Connected?* is selected as *Yes*.
3. There are up to 10 Remote Panel addresses that you could configure. These addresses are the IP Address of the Access Easy Controllers that send SMS messages via the SMS Server.

4. After the IP addresses are configured, click on the button.
5. You will need to reboot the Access Easy Controller for the changes to take effect.

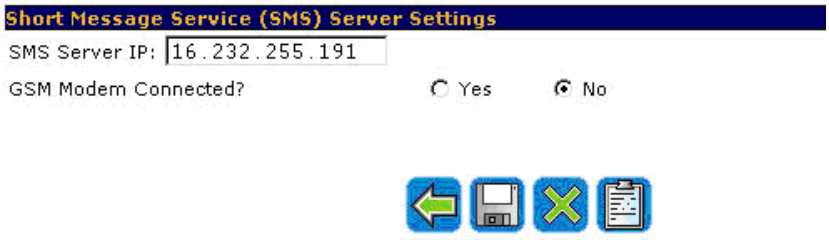
NOTICE!
To allow the Access Easy Controller that is acting as the SMS Server to send SMS message, its IP address has to be included in the list as well.

To Configure Access Easy Controller as a SMS Client

By default, the SMS Server IP address is blank. If this panel is not attached to a GSM adapter, it is a SMS Client and hence need to identify the IP Address of the SMS Server.

1. To change this setting, click on the SMS Server Settings link. The screen as shown below appears.

2. Select the No radio button for GSM Modem Connected? and click on the button. The screen as shown below appears.



3. Since this is a SMS Client, user will have to delete the default IP address in the *SMS Server IP* field and enter the IP Address of the SMS Server.
4. Click on the button.
5. You will need to reboot the Access Easy Controller for the changes to take effect.

NOTICE!

As there is only one available Serial com port in the CPU, only either the GSM adapter or the Analogue Dial-up modem can be connected to the Access Easy Controller, hence, dial-up features will not be enabled when SMS server is to be configured, like wise to the SMS server when Dial-up is been setup. By default the Dial-up feature is enabled and the SMS feature is disabled.

16.9 Reset APB

The *Reset APB* is the final menu item of the *Manual Control* Group. It allows user to reset the Anti-Passback (APB) feature once it is violated.

NOTICE!
This feature is applicable to Full and Soft Anti-Passback only.

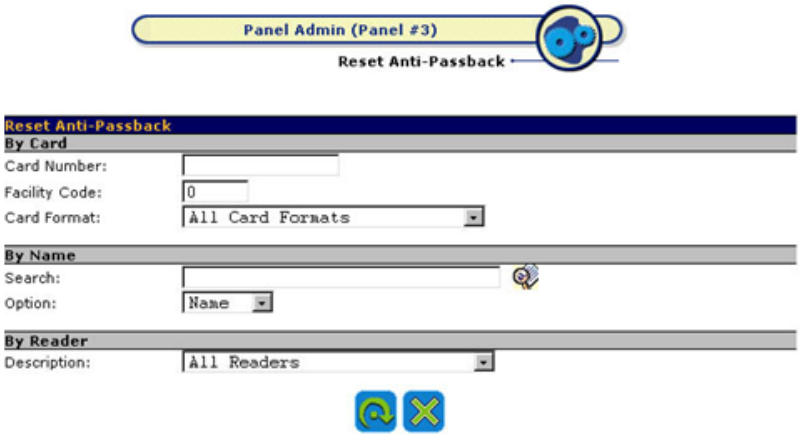
Please refer to the previous section on *How to Setup Card Readers, Anti-Passback (APB) Settings*.

If Full APB is used, this command will reset the violation and allow violator(s) to access or exit the controlled door. However, if Soft APB is used, this command will reset the Activity transactions for "Access Granted, Soft APB" and "Exit Granted, Soft APB" for violator's subsequent access or exit respectively.

User is given the option to reset the APB violation with the following combination: -

- By Card Number with respect to (wrt) Reader / All Readers, or
- By Name with respect to Reader / All Readers, or
- By All Card Numbers with respect to Reader / All Readers.

To Reset APB, select the target Access Easy Controller and click on the Reset APB hyperlink. The following page will appear in a new window.



16.9.1 How To Reset APB by Card Number wrt Reader / All Readers

To Reset APB based on Card Number, you must know the following, Card Number, its Facility Code, and its Card Format.

1. Enter the *Card Number* of the APB violator.
2. The number in the Facility Code field is configured in *Panel Setup, Default Settings*. If the code is different from the default, then change it.
3. Select the *Card Format* from the list.
4. Select the *Reader* from the list. If you want to Reset APB wrt all readers, select *All Readers*.

5. Click on the button to proceed.If the command is executed successfully, a message indicating APB reset by card & zones with respect to Reader / all Readers will be displayed.

6. Click on the button to return.

16.9.2 How to reset APB based on Name wrt Reader / All Readers

1. Enter a character, a portion, or the full name and click on the button. If a match is found that satisfies the entry, a window will appear with the names in the Names found list box. For example, enter John and click button resulted in: -

2. From the window, select the appropriate name. The selected name appears in the *Search* field.
3. Select the Readers from the list. If you want to Reset APB with respect to all readers, select *All Readers*.

4. Click on the button to proceed.

If the command is executed successfully, a message indicating APB reset will be displayed.

5. Click on the button to return.

16.9.3 How to reset APB by All Card numbers wrt Reader / All Readers

1. Select the *Readers* from the list. If you want to Reset APB with respect to all readers, select *All Readers*.

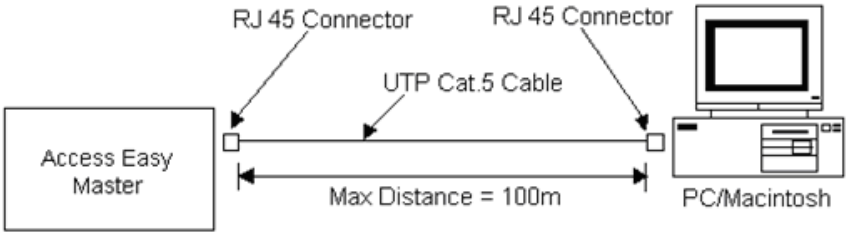
2. Click on the button to proceed.If the command is executed successfully, a message indicating APB reset by all cards & zones with respect to reader / all readers will be displayed.

3. Click on the button to return.

17 How to Configure the Access Easy Master IP Address

Configuring the IP address of the Access Easy Master requires you to initially prepare a PC/ Macintosh. This PC/Macintosh will need to have network enabled. In other words, it needs a network card pre-installed.

Refer to the figure below.



1. Connect the PC/Macintosh to the Access Easy Master with a RJ45 Cross cable.
2. Set the IP address of the PC/Macintosh to 129.2.0.40 and Subnet Mask as 255.255.0.0.

17.1 For PC Users

17.1.1 Changing the PC's IP address

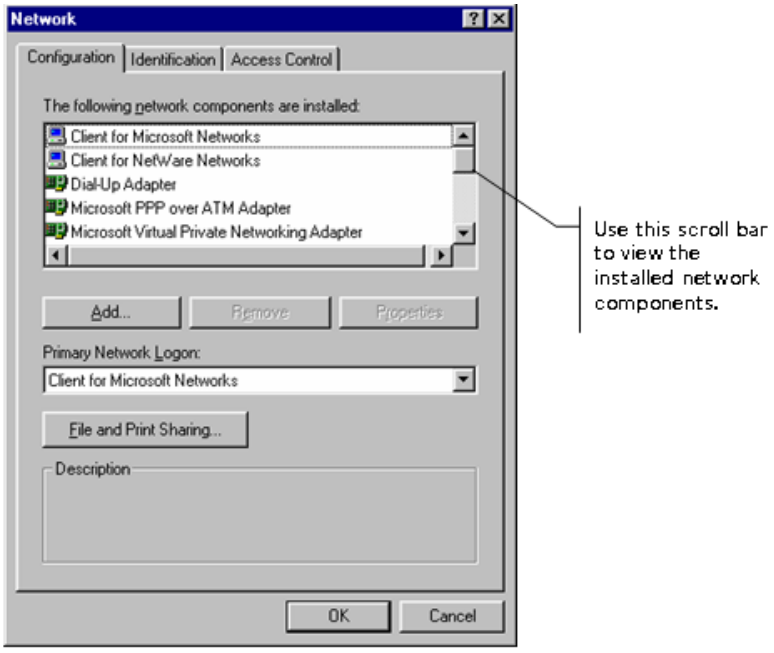
Setting the IP address of the PC is rather simple. However, if you have doubt, do ask your network administrator to assist you.

The purpose of changing the IP address of the PC is to allow it to access the Access Easy Master which has a default IP address of 129.2.0.42 (factory setting). If you do not change the IP address of the PC, you will not able to access the Access Easy Master at all. Hence it is important to have your PC pre-configured with the correct IP address before you proceed any further.

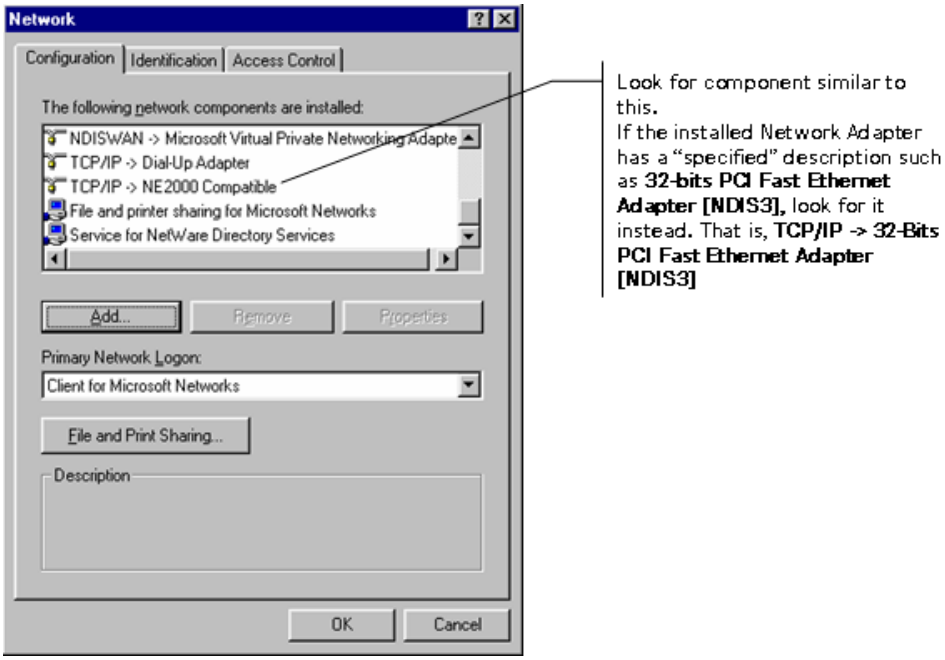
We will guide you in the following steps to configure a typical PC's IP address to 129.2.0.40. The following series of screen captures is taken with reference from Win 98. Reader should refer to their network administrator if their OS is not Win 98.

1. Click on the Start button, followed by *Settings* | *Control Panel*.

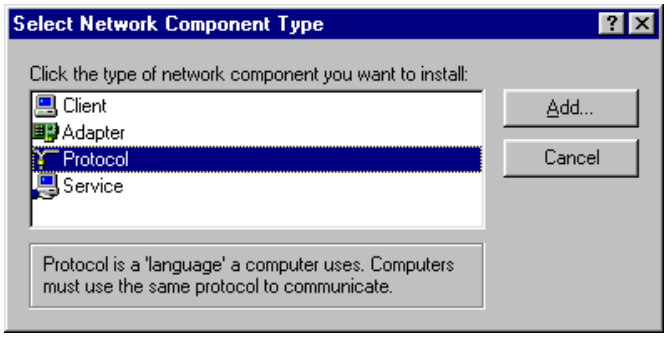
2. Double-click on the Network icon, the Network dialog box appears.



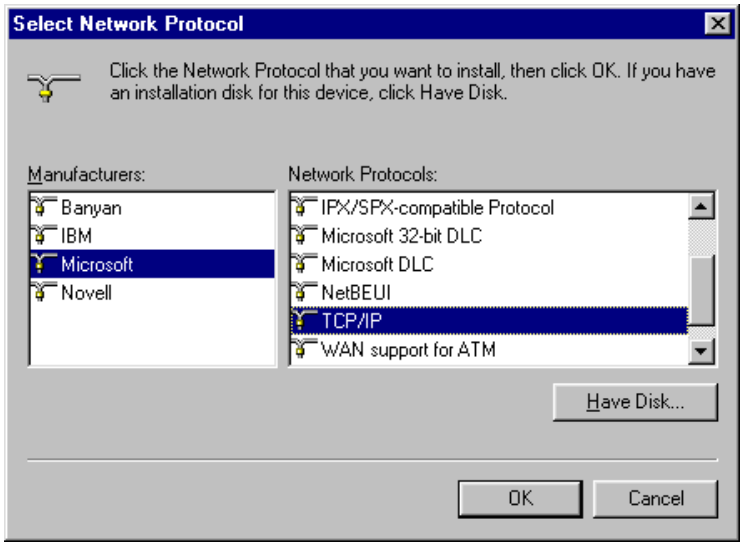
3. Use the *Scroll Bar* to look up for *TCP/IP* from the list as shown in the following diagram. However if this component is not found, proceed from step 4 to step 7 to install it, else skip to step 8.


Network
Configuration
Identification
Access Control
The following network components are installed:
NDISWAN -> Microsoft Virtual Private Networking Adapte
TCP/IP -> Dial-Up Adapter
TCP/IP -> NE2000 Compatible
File and printer sharing for Microsoft Networks
Service for NetWare Directory Services
Add...
Remove
Properties
Primary Network Logon:
Client for Microsoft Networks
File and Print Sharing...
Description
OK
Cancel
Look for component similar to this.
If the installed Network Adapter has a "specified" description such as **32-bits PCI Fast Ethernet Adapter [NDIS3],** look for it instead. That is, **TCP/IP -> 32-Bits PCI Fast Ethernet Adapter [NDIS3]**

4. To add the *TCP/IP* component, click on the Add button. The *Select Network Component Type* dialog box appears.



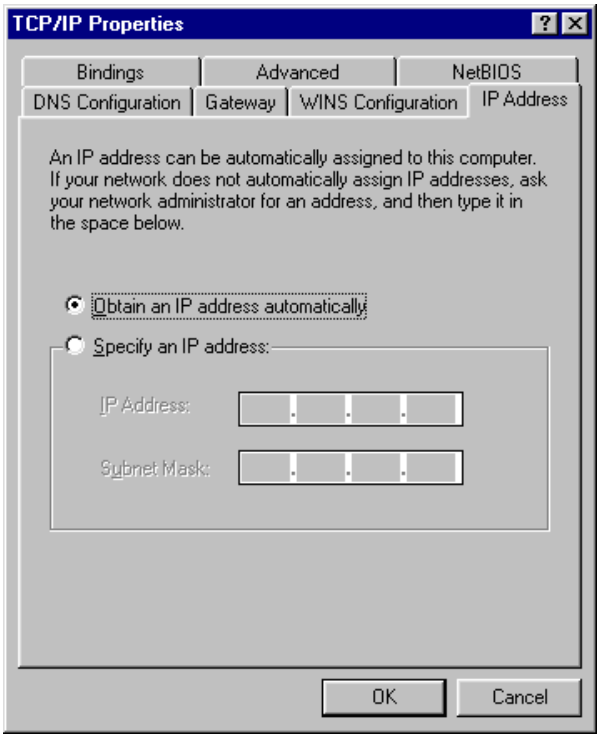
5. Click on component type Protocol and click on the Add button. The *Select Network Protocol* dialog box appears.
6. Click on *Microsoft* and *TCP/IP* as shown in the following screenshot.



7. Click on the OK button to proceed with the component installation. Follow through the on-screen instruction to complete.

NOTICE!
You might be required to have your Windows Installation Disk in your CD ROM drive.

8. Continuing from step 3, click on the Properties button. The *TCP/IP Properties* dialog box appears.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

9. Click on the Specify an IP address radio button. This will enable the field for *IP Address and Subnet Mask*.

10. Enter the *IP Address and Subnet Mask* as shown. This will be the PC's IP Address for this initial set-up.
11. Click on OK button.
12. Reboot the computer in order for the setting to take effect.

NOTICE!
The example described above is based on Windows 98 and IE5. Differences might appear for the dialog box, displays, or description if other version or different operating system is used. However, the principle of setting is the same.

17.1.2 Settings to be made to the Web browser

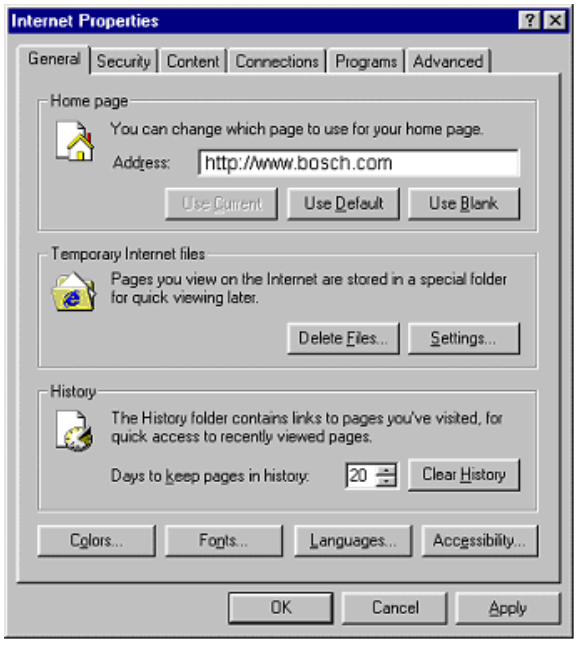
Now that you have successfully changed the PC's IP address, you will need to configure some settings on the Web browser that you intended to use to view the pages on the Access Easy Master.

Access Easy Master supports most of the popular Web browsers, such as IE5.5, Netscape4, etc. Depending on the Web browser that your PC is installed with, the following procedures will different, but the settings required are common to most Web browsers. Ask your network administrator for advice if you are unsure of where to configure these settings.

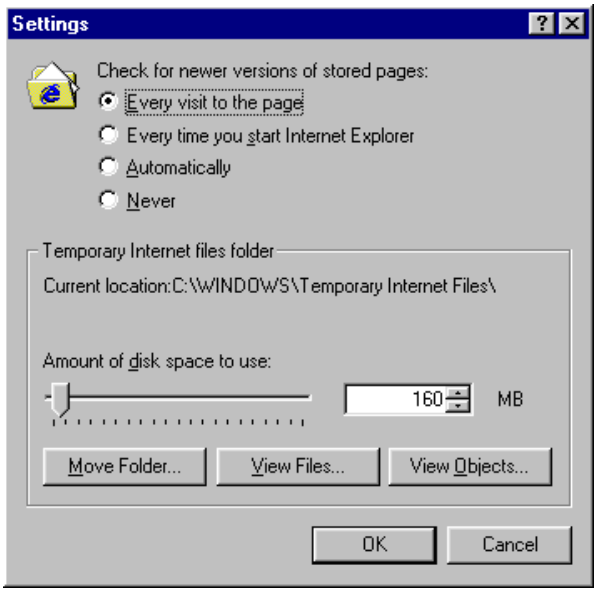
The following procedure is using IE5.5 as an example.

1. From the Windows Control Panel, click on the

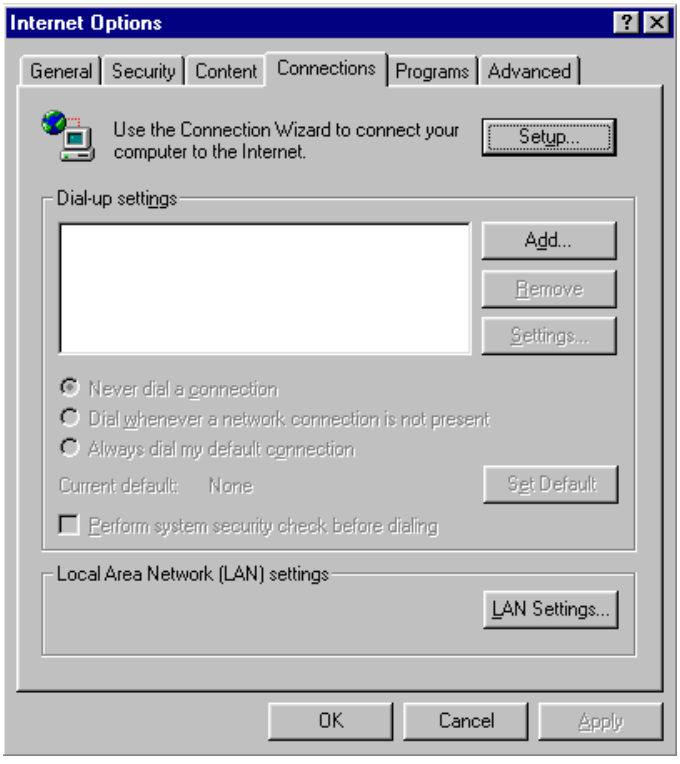
icon. The *Internet Options* dialog box appears.



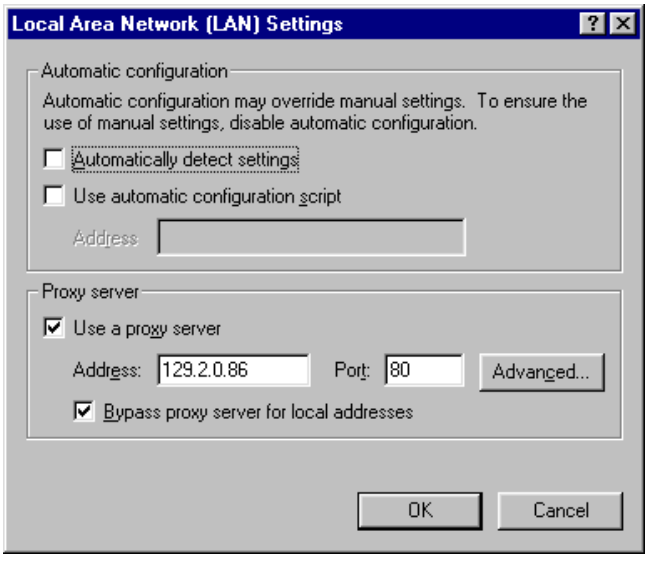
2. Under the *Temporary Internet files* heading, click on the Settings button to go into the next dialog box. Confirm that the *Check for newer versions of stored pages is set to Every visit to the page*, as shown in the following diagram. If it is not, click on the corresponding radio button. This step is necessary in order for the view in View Activity to be updated periodically.



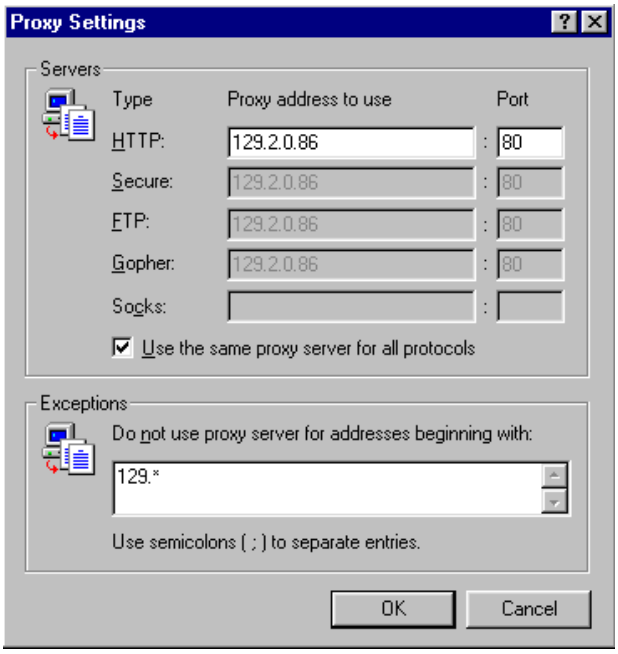
3. Click on the OK button to exit to previous dialog box.
4. If your office network does not have a Proxy Server for accessing Internet, you could skip the following steps, else please read on.



5. Under the Connections tab, click on the LAN Settings button The *LAN Settings* dialog box appears. Check on Bypass proxy Server for local addresses box if the Access Easy Master exists on the LAN.



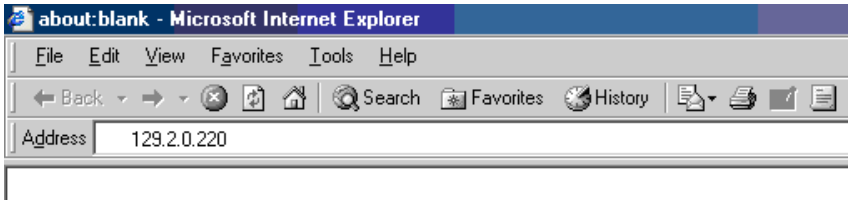
6. Click on the Advanced button. The *Proxy Settings* dialog box appears.



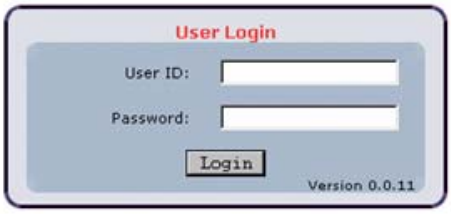
7. As shown in the above, the Proxy address used is 129.2.0.86, this is IP address of the Proxy Server in this example, it will differ in your own office. Port setting is also dependent on your office network setup. However, if this PC you are configuring has always been able to access the internet before, you will need only to enter the IP address of your Access Easy Master. Including a * like the above means to bypass the Proxy Server for all IP address starting with the 129 address.
8. Since the default IP addresses for the Access Easy Master and the Access Easy Controllers are 129.x.x.x, you may directly access the Access Easy Master and the Access Easy Controllers without going through a proxy Server. Now that the browser and IP addresses have been configured, we will now be able to view the Access Easy Master and the Access Easy Controllers through our web browser.

17.1.3 Changing the IP address of Access Easy Master

To get connected to Access Easy Master, run your web browser program and key in the Access Easy Master default URL address followed by the enter key. Please refer to the following screen shot which shows a web browser (in this case IE6 is shown) with the URL of Access Easy Master.


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address 129.2.0.220

The *User Login* dialog box appears.

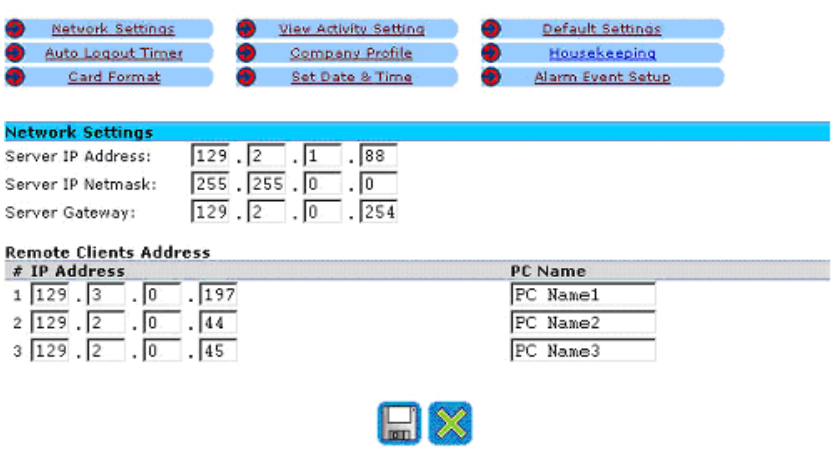


The default user id is iuser1 and the default password is 8088. The default user id is the super user id. The super user rights are assigned to the system administrator and he has full access rights over Access Easy Master. Enter the default user id and password. Now you can login to the Access Easy Master.

After getting connected to Access Easy Master, you can change the IP address of the Access Easy Master from default, to the actual IP you intend to use for the Server.

The *View Activity* page will be the first screen that the user sees after a successful login.

To change the IP address of your Access Easy Master, click on Server Setup hyperlink under *System Admin* menu in the Left Pane. By default, you will be led to the Network Settings web page. Refer to screen shot below.


Network Settings
Auto Logout Timer
Card Format
View Activity Setting
Company Profile
Set Date & Time
Default Settings
Housekeeping
Alarm Event Setup
Network Settings
Server IP Address: 129 . 2 . 1 . 88
Server IP Netmask: 255 . 255 . 0 . 0
Server Gateway: 129 . 2 . 0 . 254
Remote Clients Address
IP Address
PC Name
1 129 . 3 . 0 . 197 PC Name1
2 129 . 2 . 0 . 44 PC Name2
3 129 . 2 . 0 . 45 PC Name3

Configure the network settings for Access Easy Master by setting the appropriate IP address, subnet mask and gateway. Click on the icon at the bottom of the web page to save the new setting.

NOTICE!
Access Easy Master needs to be rebooted before the new IP address setting takes effect.

17.2 For Macintosh Users

17.2.1 Changing the Macintosh's IP address

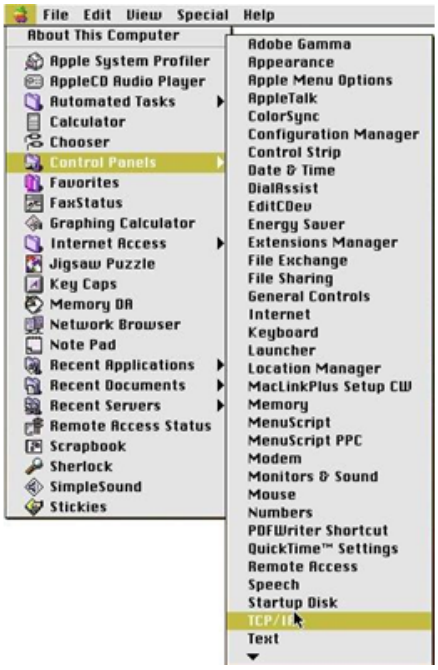
Setting the IP address of the Macintosh is rather simple. However, if you have doubt, do ask your network administrator to assist you.

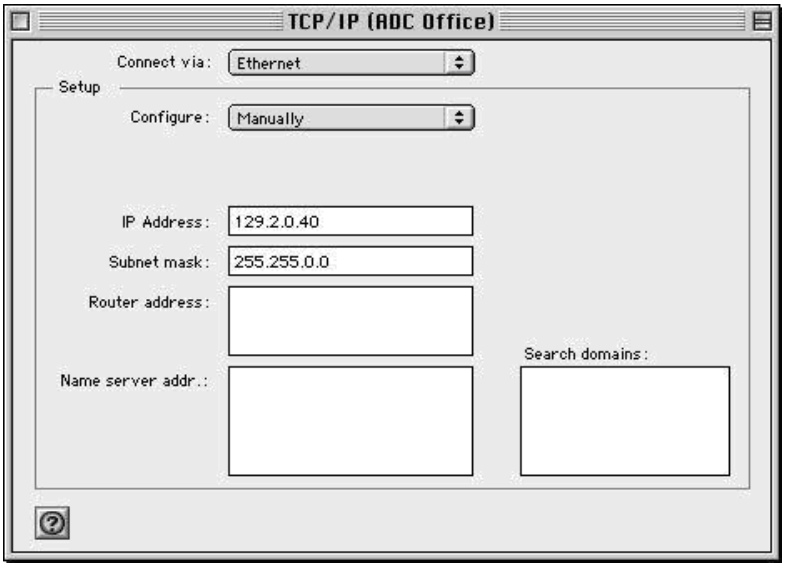
The purpose of changing the IP address of the Macintosh is to allow it to access the Access Easy Master which has a default IP address of 129.2.0.42 (factory setting). If you do not change the IP address of the Macintosh, you will not able to access the Access Easy Master at all. Hence it is important to have your Macintosh pre-configured with the correct IP address before you proceed any further.

We will guide you in the following steps to configure a typical Macintosh's IP address to 129.2.0.40.

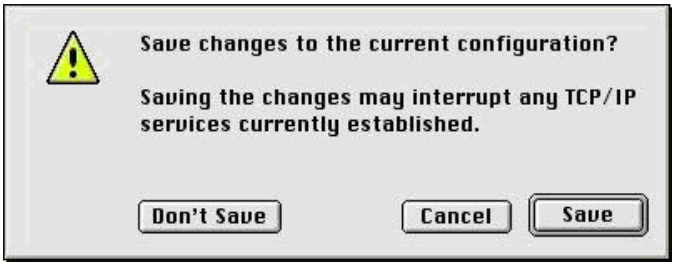
Follow through the procedures to set the IP Address for the Macintosh.

1. Click on the Apple icon to show a list of control function.
2. Select *Control Panels, TCP/IP*. The *TCP/IP* dialog box appears.





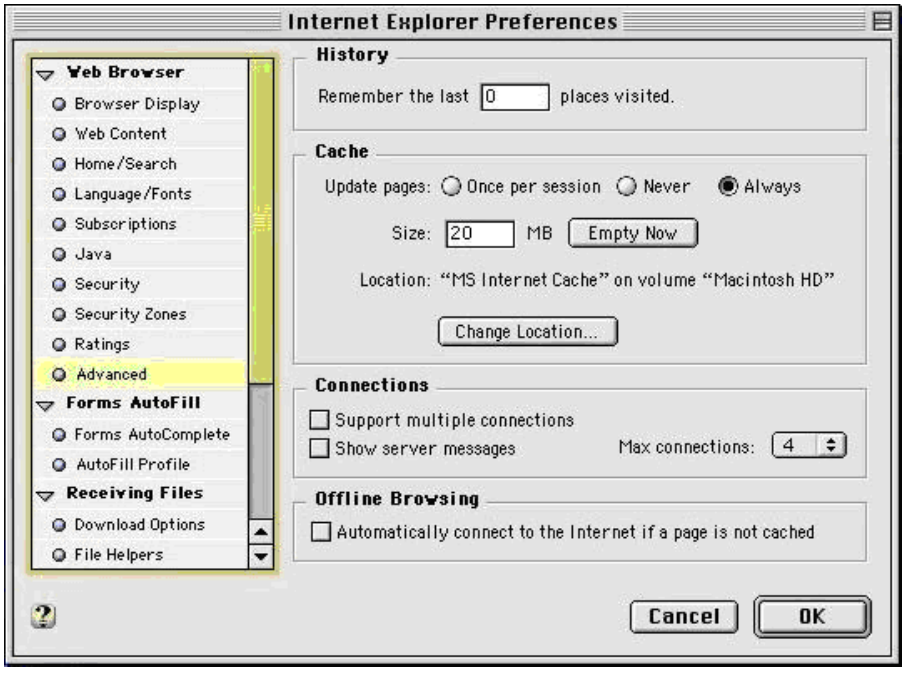
3. Enter the *IP Address* and the *Subnet mask* as shown above. This will be the Macintosh's IP Address for this initial set-up.
4. Click on the Save button when prompted. This message will appear when you attempt to close the dialog box.


Save changes to the current configuration?
Saving the changes may interrupt any TCP/IP services currently established.
Don't Save
Cancel
Save

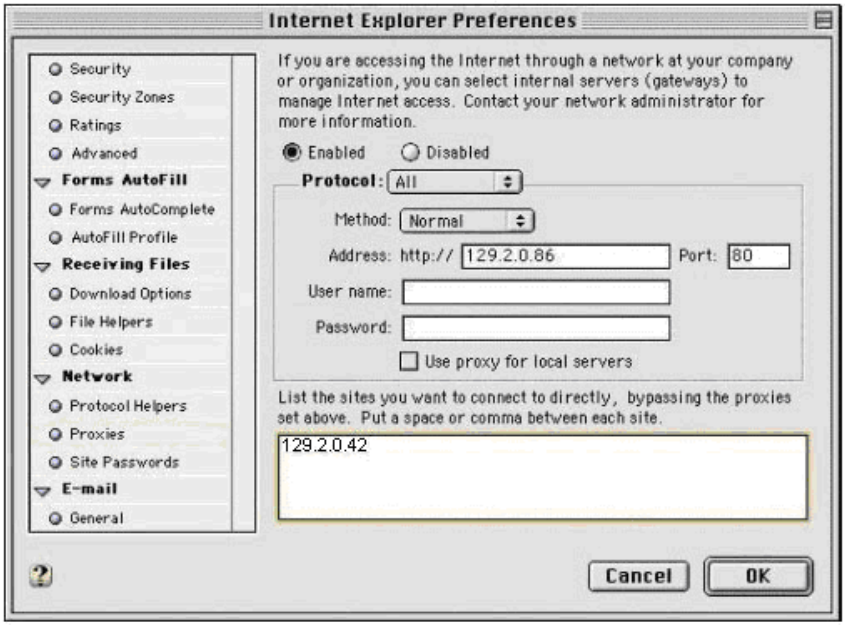
17.2.2 Settings to be made to the Web browser

1. Launch the Internet Explorer for Macintosh.
2. From the Toolbars, click on Preferences.
3. Under Web Browser, select *Advanced* (see diagram below).

4. Select Update pages - Always for Cache.

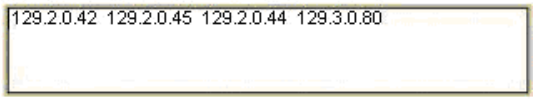


5. Use the Scrollbar to scroll down the listing to look for *Proxies*.



6. Enter the Access Easy Master default IP Address into the box as shown above. IP Addresses enter here will bypass the proxies and connect directly.

7. If the IP Address of the Access Easy Controllers have been assigned, continue to enter the addresses in the field, separating each Address by a space or a comma. The screen-capture shows the Default IP Address for Access Easy Master and three assigned Access Easy Controllers IP Addresses, 129.2.0.45, 129.2.0.44, and 129.3.0.80.



8. Click on the OK button to close the dialog box. With this settings done, we can proceed to access the Access Easy Master. To change the IP address of the Access Easy Master, follow the steps in the section *Changing the IP address of Access Easy Master* above. Changing the IP address of the Access Easy Master on the Macintosh is the same as changing it on the PC.

18 Accessing and Understanding Access Easy for Master Main Menu

In this chapter, you will learn the basic information of how to access the and logging onto the Access Easy for Master software.

Access Easy for Master Software GUI is the same as Access Easy Controller Software GUI BUT Access Easy for Master Software only support minimal functions as most of the functions are centrally administer and control by Access Easy Master Software.

In order to operate one or more Controller from one or more computers, a standard web browser program such as *Internet Explorer, version 4.0 and above, or Netscape Navigator, version 4.0* and above on each of the central monitoring computer is required.

18.1 Connecting to Access Easy for Master

Before the Access Easy for Master can be access, it must be configured properly and integrated to the existing computer network.

As this integration is fairly complex and requires knowledge on networking, it is the responsibility of the *System Installer* to working closely with your company's *Network Administrator* to do the initial set up.

However, for general knowledge, a description is presented in *Appendix F*.

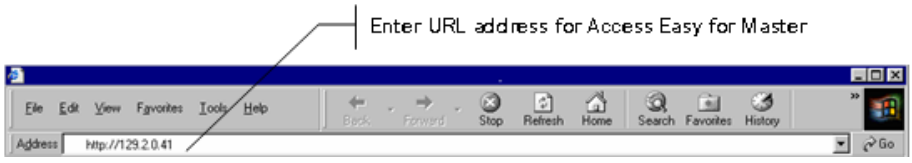
For users accessing the using their own computer, please read up on the section *Setting to be made to the Web Browser*.

18.2 Logging onto Access Easy for Master

A working knowledge of Windows or Macintosh and the standard web browser program, either Internet Explorer or Netscape Navigator and the ability to manoeuvre with a mouse pointer is required to complete the appropriate screen.

To get connected to Access Easy for Master, run your web browser program and key in the Access Easy for Master's URL address followed by the Enter key.

The following screen-capture shows example of some typical web browser page with the default URL address for the Access Easy for Master. The outlook of the screen might differ from what is shown here, this is largely due to the software version in use.


Enter URL address for Access Easy for Master
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History
Address http://129.2.0.41
Go

This is a sample of how the screen would look like for user using *Internet Explorer*.

The *User Login* dialog box appears.

This *User Login* dialog box provides a security control that protects the Access Easy for Master from unauthorised access. It requires a user to enter his or her *User ID* followed by a *Password* before he or she is allowed access to Access Easy for Master. Up to two users are able to log onto the same Access Easy for Master concurrently using different computers.

NOTICE!
The Password is case-sensitive and can be changed.

The Access Easy for Master has only one assigned User ID and Password. This default *User ID* has only restricted access rights to all features of the Access Easy for Master. The *User ID* and *Password* can be changed.

The default User ID = user1 and Password = 8088

NOTICE!
Once the system is commissioned and handed-over, change the default User ID and Password as soon as possible to prevent unauthorised access.

18.2.1 Logging onto Access Easy for Master

1. Enter your assigned *User ID* in the *User ID* edit box.
2. Enter your assigned *Password*.
3. Click on the *Login* button.

If you do not know your User ID and Password, contact your System Administrator to obtain them. User IDs and Passwords are only configured by the Access Easy for Master System Administrator.

18.2.2 Logging off from Access Easy for Master

After you finish your session with Access Easy for Master or need to be away from the computer, it is recommended to log off from the Access Easy for Master.
To log off, click on the *Logout* link. Click on the appropriate button to proceed.

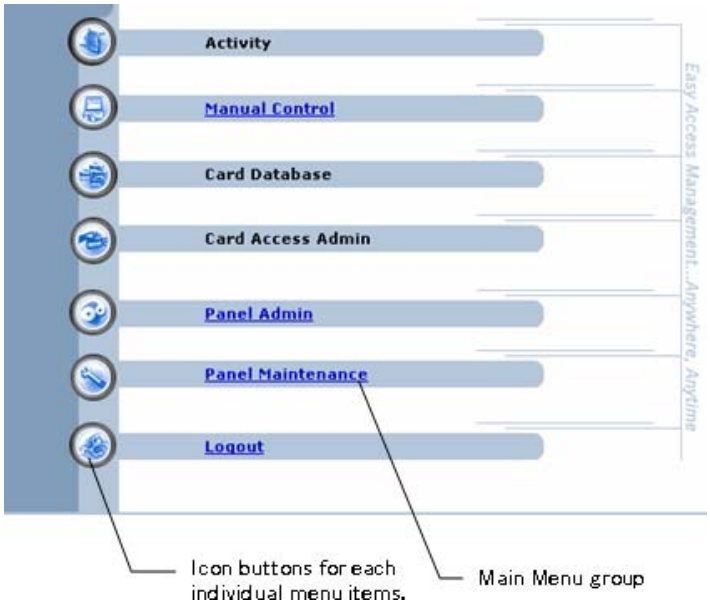
18.3 Understanding the Home Page Main Menu Groups

The *Home* Page gives an overview of the main functional features that the Access Easy for Master supports and does not contain any parameters setting or data.

For the user convenience, the icon buttons, in line to the main menu group, is linked to the page of the first menu item in the group.

Once in the menu item page, the *Home* page icon button is added to the bottom of the list after the Logout button. This is good for security reason. Should a user is suddenly disrupted while in a middle of setting the Access Easy for Master parameters, for example to answer a phone call, he or she can click the *Home* button to exit the setting without having to click a few times on the *Back* button. This will prevent prying-eyes from looking at the setting.

The screen-capture shown below shows the Home page.



Only minimal features are available to Access Easy for Master. Details of the various menu items that are available for Access Easy for Master will be covered in the next following chapters. However, a brief description of each item will be presented here.

NOTICE!
Most of the features are incorporated into Access Easy Master. This allows Access Easy Master to centrally control and administer all changes of the Access Easy Controller.

18.3.1 Manual Control

This menu group relates more to manual (user intervention) control of system hardware and consists of the following menu items: Door Control, Input Control, Output Control, and Reset APB.

18.3.2 Panel Admin

Users are to set-up the User ID and Password including access rights to the various menu items.

Panel Setup is for setting up of various miscellaneous parameters: -

- Network Settings
- Auto Logout Timer
- Audit Log
- Set Date & Time

18.3.3 Panel Maintenance

Update Flash is a utility that is used when there is a program upgrade. It's usually carried out for firmware enhancement, new features, or bug fixing.
It can also be used for database recovery.

Reboot Panel is used to reboot the Access Easy for Master. It's usually carried out before changes can take effect. Some examples are Access Easy for Master IP Address or during a firmware upgrade.

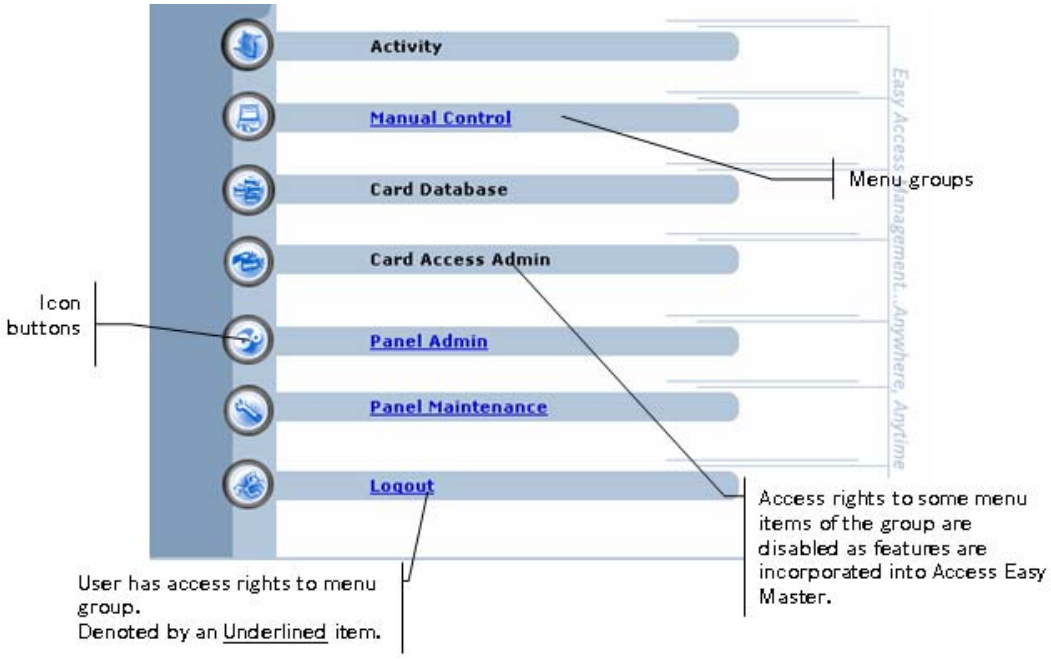
18.3.4 Logout

To log off from Access Easy for Master.

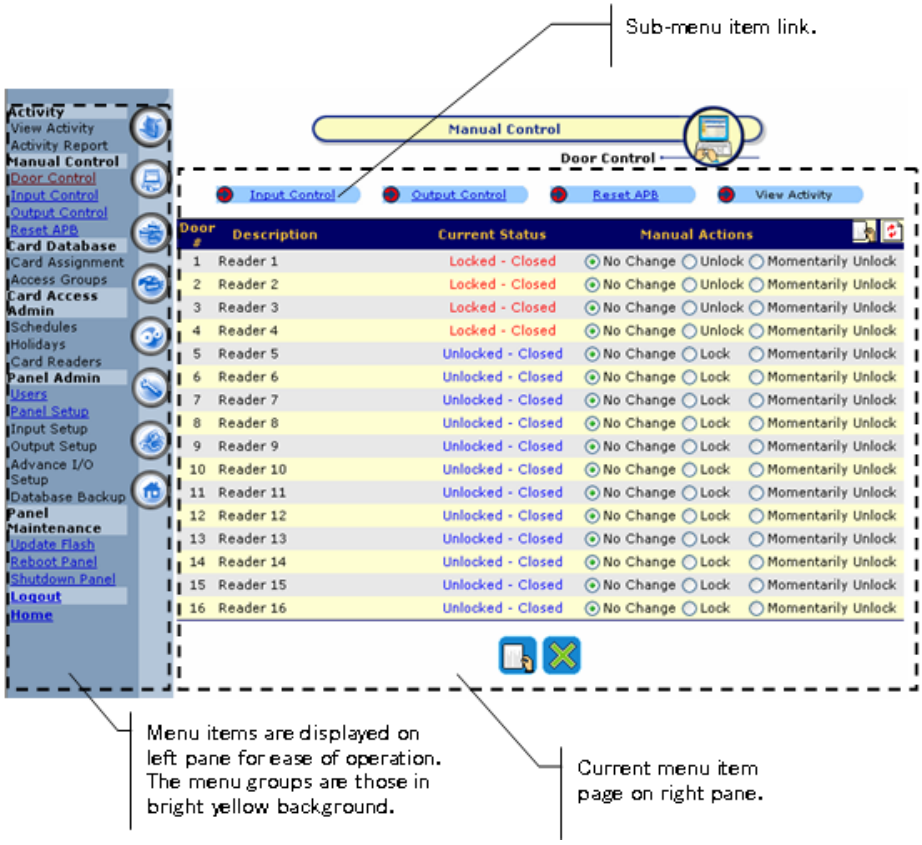
18.4 Navigating Through Access Easy for Master page

The following screen-capture shows some sample pages indicating how you can navigate through Access Easy for Master software.

Home Page


Activity
Manual Control
Card Database
Card Access Admin
Panel Admin
Panel Maintenance
Logout
Menu groups
Icon buttons
Access rights to some menu items of the group are disabled as features are incorporated into Access Easy Master.
User has access rights to menu group.
Denoted by an Underlined item.

Clicking on an Underlined menu group would bring you to the first available access-right-menu item web page in the group.

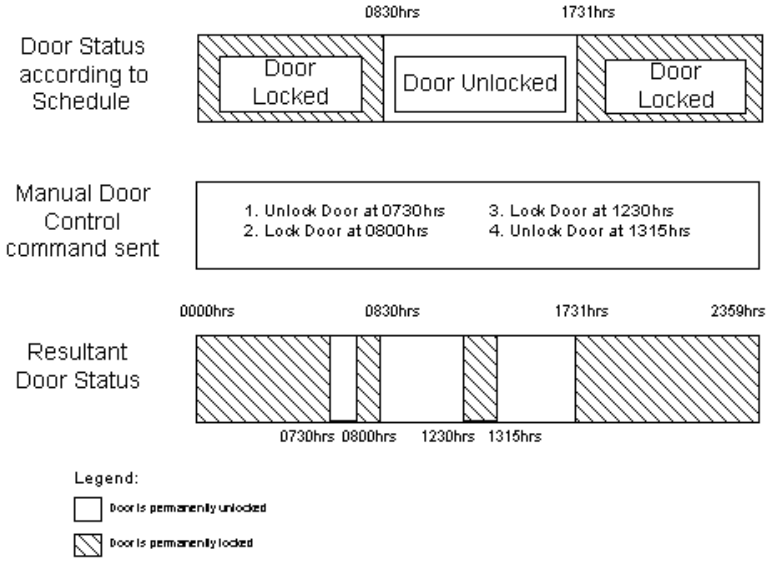

Sub-menu item link.
Activity
View Activity
Activity Report
Manual Control
Door Control
Input Control
Output Control
Reset APB
Card Database
Card Assignment
Access Groups
Card Access
Admin
Schedules
Holidays
Card Readers
Panel Admin
Users
Panel Setup
Input Setup
Output Setup
Advance I/O
Setup
Database Backup
Panel
Maintenance
Update Flash
Reboot Panel
Shutdown Panel
Logout
Home
Manual Control
Door Control
Input Control
Output Control
Reset APB
View Activity
Door #
Description
Current Status
Manual Actions
1 Reader 1 Locked - Closed No Change Unlock Momentarily Unlock
2 Reader 2 Locked - Closed No Change Unlock Momentarily Unlock
3 Reader 3 Locked - Closed No Change Unlock Momentarily Unlock
4 Reader 4 Locked - Closed No Change Unlock Momentarily Unlock
5 Reader 5 Unlocked - Closed No Change Lock Momentarily Unlock
6 Reader 6 Unlocked - Closed No Change Lock Momentarily Unlock
7 Reader 7 Unlocked - Closed No Change Lock Momentarily Unlock
8 Reader 8 Unlocked - Closed No Change Lock Momentarily Unlock
9 Reader 9 Unlocked - Closed No Change Lock Momentarily Unlock
10 Reader 10 Unlocked - Closed No Change Lock Momentarily Unlock
11 Reader 11 Unlocked - Closed No Change Lock Momentarily Unlock
12 Reader 12 Unlocked - Closed No Change Lock Momentarily Unlock
13 Reader 13 Unlocked - Closed No Change Lock Momentarily Unlock
14 Reader 14 Unlocked - Closed No Change Lock Momentarily Unlock
15 Reader 15 Unlocked - Closed No Change Lock Momentarily Unlock
16 Reader 16 Unlocked - Closed No Change Lock Momentarily Unlock
Menu items are displayed on left pane for ease of operation. The menu groups are those in bright yellow background.
Current menu item page on right pane.

19 Door Control

The Door Control is one of the menu items of the Manual Control Group. It allows user to check the status of all the doors and send a command to either momentarily unlock or permanently unlock / lock the door without having to be at the door location.

As this is a control operated by a user manually, it has priority over the control set by the system. However, the system will take over and resume normal operation once it encounters a valid Schedule Interval.

We show an example to illustrate the condition.
The setting for Interval 1 is Start - 0830hrs and End - 1730hrs.
Interval 2,3, and 4 has no setting.

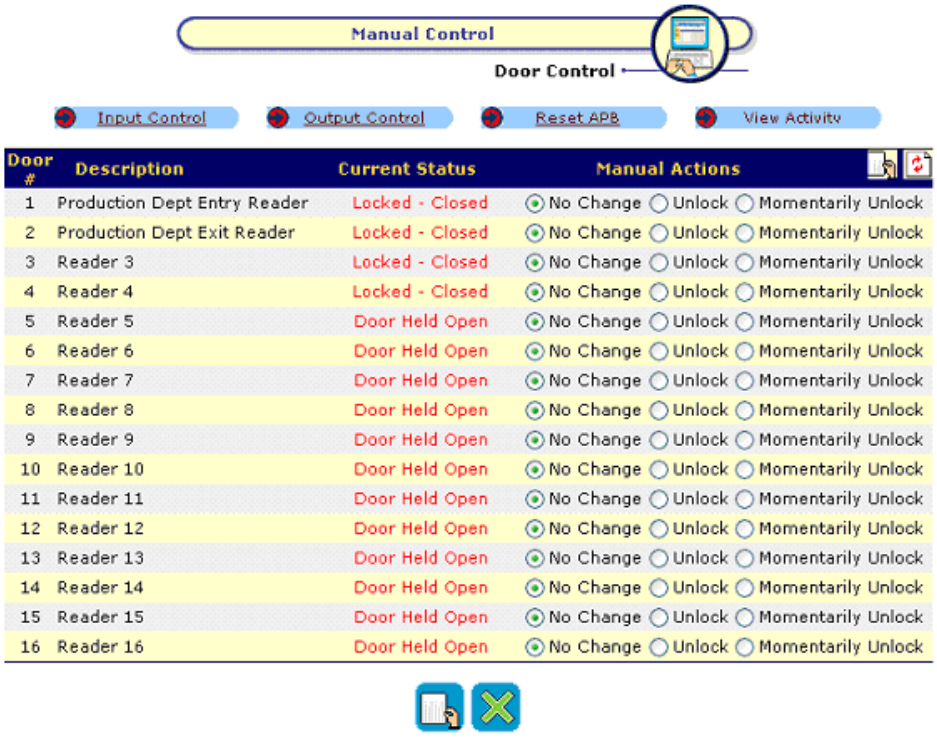


Notice that the system resume normal operation as according to Schedule at 0830hrs and 1731hrs.

19.1 To activate Door Control

There are various ways to activate the Door Control menu item. They are: -

1. From the Home page, click on Manual Control or its icon button.
2. From the View Activity page, click on Door Control hyperlink.
3. From any of the menu items page of the Manual Control Group.


Manual Control
Door Control
Input Control
Output Control
Reset APB
View Activity
Door #
Description
Current Status
Manual Actions
1 Production Dept Entry Reader Locked - Closed No Change Unlock Momentarily Unlock
2 Production Dept Exit Reader Locked - Closed No Change Unlock Momentarily Unlock
3 Reader 3 Locked - Closed No Change Unlock Momentarily Unlock
4 Reader 4 Locked - Closed No Change Unlock Momentarily Unlock
5 Reader 5 Door Held Open No Change Unlock Momentarily Unlock
6 Reader 6 Door Held Open No Change Unlock Momentarily Unlock
7 Reader 7 Door Held Open No Change Unlock Momentarily Unlock
8 Reader 8 Door Held Open No Change Unlock Momentarily Unlock
9 Reader 9 Door Held Open No Change Unlock Momentarily Unlock
10 Reader 10 Door Held Open No Change Unlock Momentarily Unlock
11 Reader 11 Door Held Open No Change Unlock Momentarily Unlock
12 Reader 12 Door Held Open No Change Unlock Momentarily Unlock
13 Reader 13 Door Held Open No Change Unlock Momentarily Unlock
14 Reader 14 Door Held Open No Change Unlock Momentarily Unlock
15 Reader 15 Door Held Open No Change Unlock Momentarily Unlock
16 Reader 16 Door Held Open No Change Unlock Momentarily Unlock

The following paragraphs provide some description of what will you see on the web page.

Current Status: provide user with the current status of the door. There are 5 door control status.

Status	Description
Locked - Closed	Indicates that the door is locked permanently.
Unlocked - Open	Indicates that the door is unlocked and open.
Unlocked - Closed	Indicates that the door is unlocked and close.
Door Forced Open	Indicates that door is forced open.
Door Held Open	Indicates that door is held open beyond a period of time(Exceeded the time settings of Door Open Timer)

Manual Actions: provide user with radio buttons selection of what manual action to perform.

The description of the second radio button is the opposite of the current status and it will toggle between Lock and Unlock.

The third radio button, *Momentary Unlock*, is used to send a command to momentarily unlocked the door for a duration as specified by the *Door Strike Timer*. This command is only effective when the current status of the door is Locked.

19.1.1 To control the Doors manually

1. Select the desired action radio button(s) (see NOTICE 1).

2. Click on either or button to send the command.

The web page will refresh to reflect the new status.

NOTICE!

1. Select only door(s) that you want to send command to.

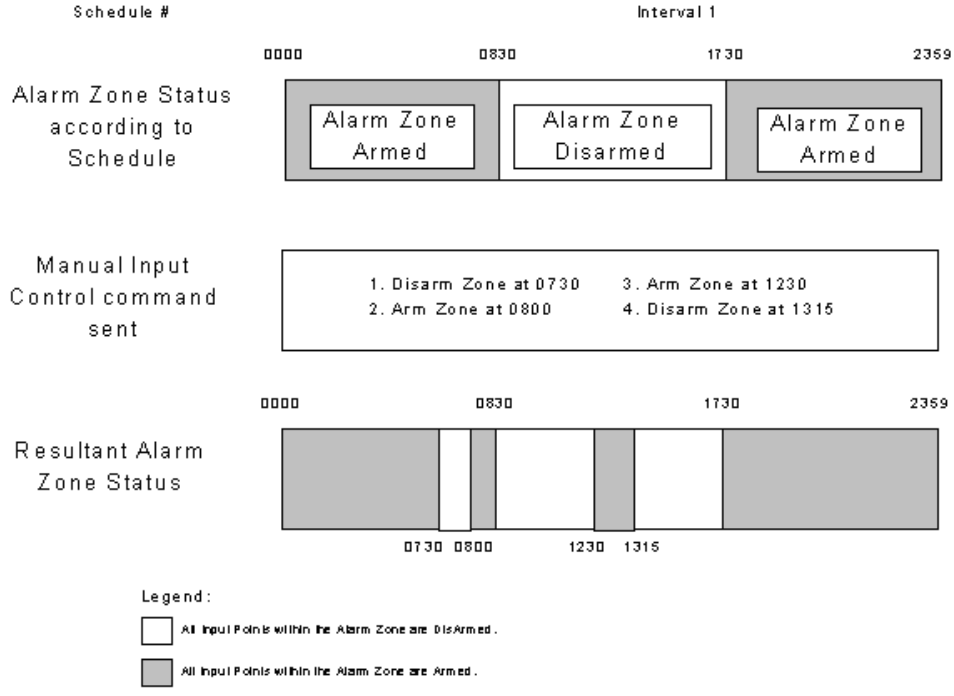
2. The current status of the door for a Momentarily Unlocked command will not show the true status after the *Door Strike Timer* has elapsed, unless the user refreshes the web page by click on the button.

20 Input Control

The Input Control is one of the menu items of the Manual Control Group. It allows user to check the status of all the Input Points assigned to specific Alarm Zones and to send a command to Arm / Disarm the Zone manually.

As this is a control operated by a user manually, it has priority over the control set by the system. However, the system will take over and resume normal operation once it encounters a valid Schedule Interval.

Before we begin, we show an example to illustrate the operational behaviour. The setting for Interval 1 is Start - 0830hrs and End - 1730hrs.
Interval 2,3, and 4 has no setting.

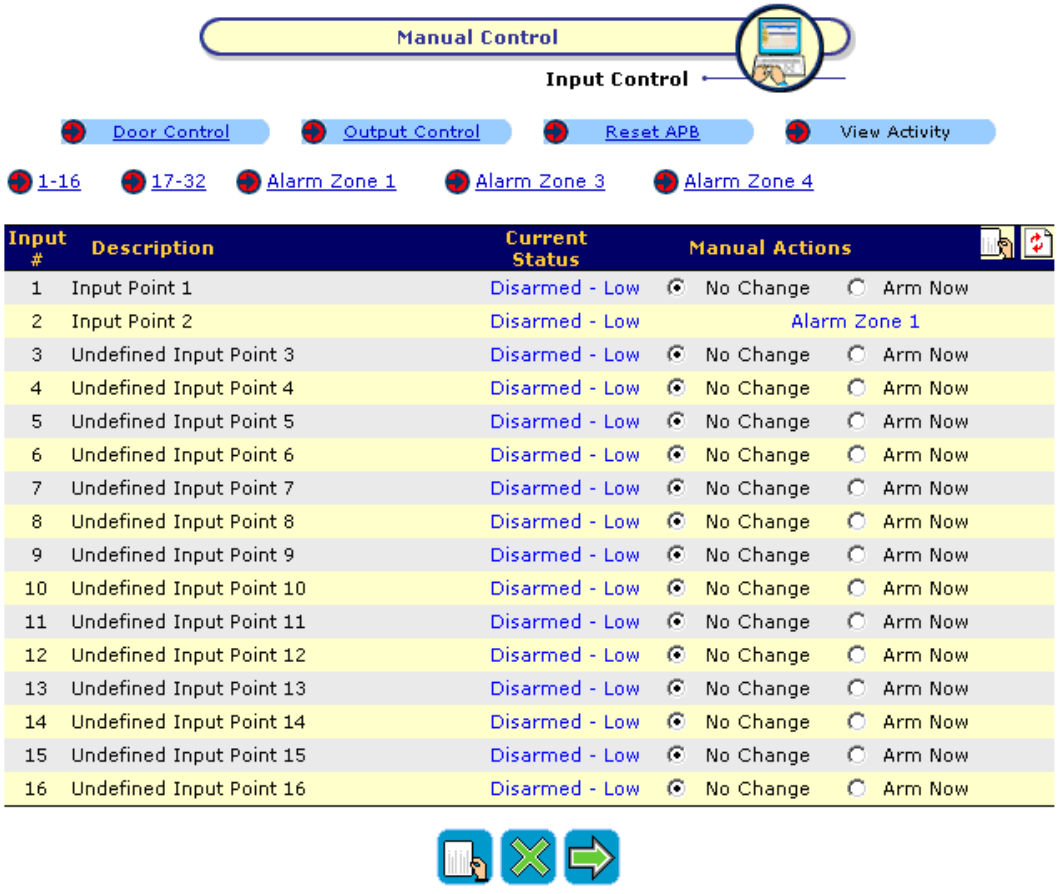


Notice that the system resumes normal operation as according to Schedule at 0830hrs and 1731hrs.

20.1 To activate Input Control

There are various ways to activate the Input Control. They are: -

1. From any menu item page, click on Input Control hyperlink.
2. From the View Activity page, click on Input Control hyperlink.
3. From any of the menu items page of the Manual Control Group.



Input #	Description	Current Status	Manual Actions
1	Input Point 1	Disarmed - Low	No Change / Arm Now
2	Input Point 2	Disarmed - Low	Alarm Zone 1
3	Undefined Input Point 3	Disarmed - Low	No Change / Arm Now
4	Undefined Input Point 4	Disarmed - Low	No Change / Arm Now
5	Undefined Input Point 5	Disarmed - Low	No Change / Arm Now
6	Undefined Input Point 6	Disarmed - Low	No Change / Arm Now
7	Undefined Input Point 7	Disarmed - Low	No Change / Arm Now
8	Undefined Input Point 8	Disarmed - Low	No Change / Arm Now
9	Undefined Input Point 9	Disarmed - Low	No Change / Arm Now
10	Undefined Input Point 10	Disarmed - Low	No Change / Arm Now
11	Undefined Input Point 11	Disarmed - Low	No Change / Arm Now
12	Undefined Input Point 12	Disarmed - Low	No Change / Arm Now
13	Undefined Input Point 13	Disarmed - Low	No Change / Arm Now
14	Undefined Input Point 14	Disarmed - Low	No Change / Arm Now
15	Undefined Input Point 15	Disarmed - Low	No Change / Arm Now
16	Undefined Input Point 16	Disarmed - Low	No Change / Arm Now

This is the View Status page. It allows user to view the current status of all assigned Input Points and the respective Alarm Zone the Input Points belongs to.

NOTICE!
Only Input Points that are not controlled specifically based on Schedule will be shown on the web page.

Description provides the grouping of the Input Point, if any. The horizontal strip in blue provides the Alarm Zone to which the Input Points belong. The Alarm Zones are separated by a blue line. Independent Input Points do not belong to any Alarm Zone. In this case, Input Point 2 belongs to Alarm Zone 1. Input Point 1 is an independent input point.

The table below describes the possible grouping of the Input Point.

Alarm Zone 1	Input Points in Alarm Zone 1 are displayed together. They are to be armed / disarmed together.
Alarm Zone 2	Input Points in Alarm Zone 2 are displayed together. They are to be armed / disarmed together.
Alarm Zone 3	Input Points in Alarm Zone 3 are displayed together. They are to be armed / disarmed together.
Alarm Zone 4	Input Points in Alarm Zone 4 are displayed together. They are to be armed / disarmed together.
Independent Input Point	These are Independent Input Points which can be armed / disarmed by itself.

Current Status column provides us with the current input point status.

The table below describes the possible status of the Input Point.

Current Status	Description
Armed	The respective Input Point is Armed.
Disarmed - Low	The respective Input Point is Disarmed and its current status is close.
Disarmed - High	The respective Input Point is Disarmed and its current status is open.
Alarm	An Alarm is detected from the Input Point.
Bypassed - Low	The Input Point has been bypassed though the alarm zone is armed. This situation can only happen when the input point status is close while the alarm zone is armed.
Bypassed - High	The Input Point has been bypassed though the alarm zone is armed. This situation can only happen when the input point status is open while the alarm zone is armed.

Manual Actions column provides the check box for selection of the input points to issue the command.

There are 2 types of action command available:

	This icon means that by selecting the check box, an Arming command will be issued when submitted.
	This icon means that by selecting the check box, a Disarming command will be issued when submitted.

20.1.1 To control (Arm/Disarm) an Input Point

These are Input points that are not included in any of the 4 Alarm Zones nor are it controlled by Schedule. They are independent points that could be armed or disarmed manually.

Manual Control
Input Control
Door Control
Output Control
Reset APB
View Activity
1-16
17-32
Alarm Zone 1
Alarm Zone 3
Alarm Zone 4
Input # Description Current Status Manual Actions
1 Input Point 1 Disarmed - Low No Change Arm Now
2 Input Point 2 Disarmed - Low Alarm Zone 1
3 Undefined Input Point 3 Disarmed - Low No Change Arm Now
4 Undefined Input Point 4 Disarmed - Low No Change Arm Now
5 Undefined Input Point 5 Disarmed - Low No Change Arm Now
6 Undefined Input Point 6 Disarmed - Low No Change Arm Now
7 Undefined Input Point 7 Disarmed - Low No Change Arm Now
8 Undefined Input Point 8 Disarmed - Low No Change Arm Now
9 Undefined Input Point 9 Disarmed - Low No Change Arm Now
10 Undefined Input Point 10 Disarmed - Low No Change Arm Now
11 Undefined Input Point 11 Disarmed - Low No Change Arm Now
12 Undefined Input Point 12 Disarmed - Low No Change Arm Now
13 Undefined Input Point 13 Disarmed - Low No Change Arm Now
14 Undefined Input Point 14 Disarmed - Low No Change Arm Now
15 Undefined Input Point 15 Disarmed - Low No Change Arm Now
16 Undefined Input Point 16 Disarmed - Low No Change Arm Now
Input Points that does not belongs to any Alarm Zone

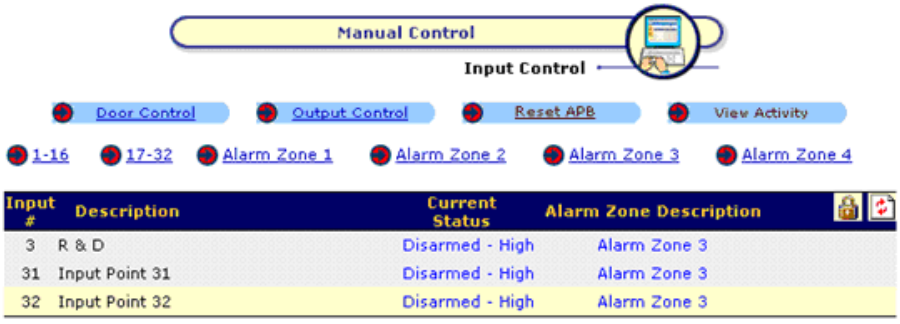
1. Click on the appropriate link, 1-16 or 17-32 , to display the correct range of Input Points. Alternatively, you can click on the or button.
2. Select the desired radio button(s) (see NOTICE).
3. Click on either or button to send the command. The web page will refresh to reflect the new status.

NOTICE!

If the current status of the Input Point is Armed, the Manual Action will shows Disarm Now which means you could send a disarm command to this input when the button is click. Likewise, if the Input Point is currently Disarmed, the Manual Action will shows Arm Now

20.1.2 To control (Arm/Disarm) the Alarm Zone

1. Click on the appropriate Alarm Zone link to display the list of Input Points configured to that zone. For example, click on the Alarm Zone 3 link will only list those Input Points configured for Alarm Zone 3 as shown below.



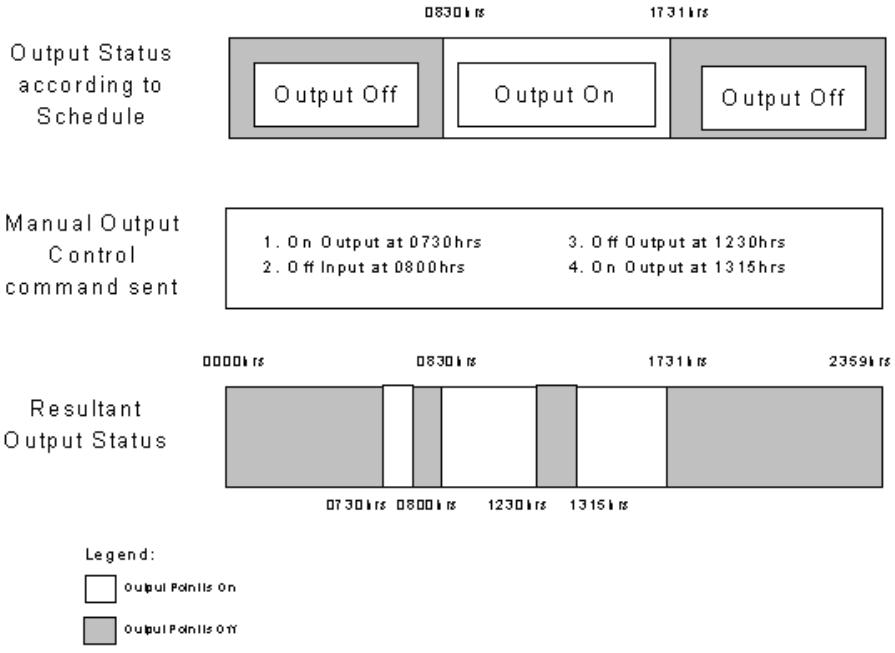
2. Click on the button to arm the Input Points within the Alarm Zone. The web page will refresh to reflect the new status and the button changes to , clicking on it will Disarm all the Input Points within the Alarm Zone.

21 Output Control

The Output Control is one of the menu items of the Manual Control Group. It allows user to check the status of all the Output Points and send a command to turn On / Off the points manually. However, if the Output Point is linked to an Input Point as a Status Output, the status will not be indicated here.

As this is a control operated by a user manually, it has priority over the control set by the system. However, the system will take over and resume normal operation once it encounters a valid Schedule Interval.

Before we begin, we show an example to illustrate the operational condition
The setting for Interval 1 is Start - 0830hrs and End - 1730hrs.
Interval 2,3, and 4 has no setting.

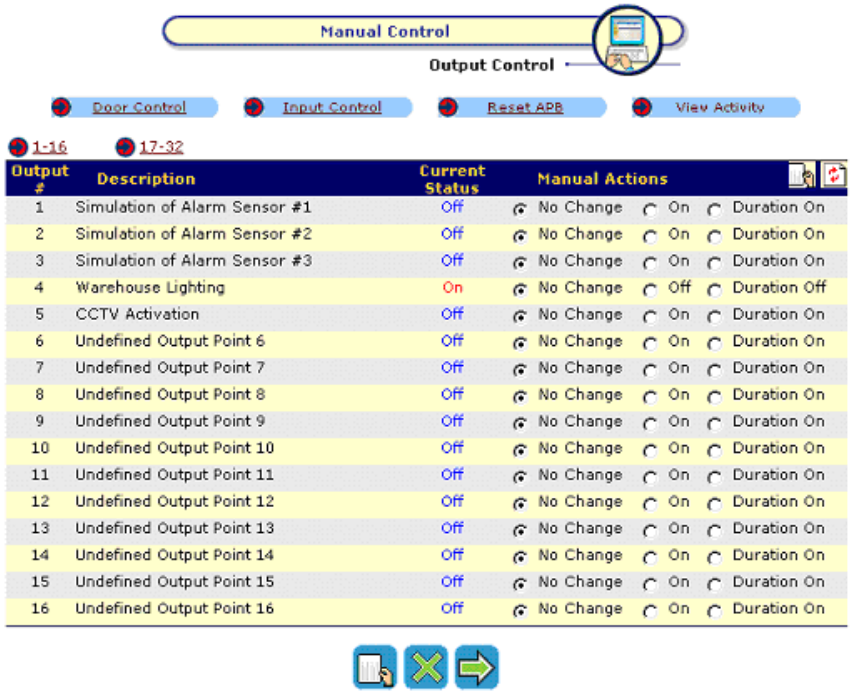


Notice that the system resumes normal operation as according to Schedule at 0830hrs and 1731hrs.

21.1 To activate Output Control

There are various ways to activate the Output Control. They are: -

1. From any menu item page, click on Output Control hyperlink.
2. From the View Activity page, click on Output Control hyperlink.
3. From any of the menu items page of the Manual Control Group.



Output #	Description	Current Status	Manual Actions
1	Simulation of Alarm Sensor #1	Off	No Change / On / Duration On
2	Simulation of Alarm Sensor #2	Off	No Change / On / Duration On
3	Simulation of Alarm Sensor #3	Off	No Change / On / Duration On
4	Warehouse Lighting	On	No Change / Off / Duration Off
5	CCTV Activation	Off	No Change / On / Duration On
6	Undefined Output Point 6	Off	No Change / On / Duration On
7	Undefined Output Point 7	Off	No Change / On / Duration On
8	Undefined Output Point 8	Off	No Change / On / Duration On
9	Undefined Output Point 9	Off	No Change / On / Duration On
10	Undefined Output Point 10	Off	No Change / On / Duration On
11	Undefined Output Point 11	Off	No Change / On / Duration On
12	Undefined Output Point 12	Off	No Change / On / Duration On
13	Undefined Output Point 13	Off	No Change / On / Duration On
14	Undefined Output Point 14	Off	No Change / On / Duration On
15	Undefined Output Point 15	Off	No Change / On / Duration On
16	Undefined Output Point 16	Off	No Change / On / Duration On

The following paragraphs provide some description of what you will see on the web page.

Current Status: provide user with the current status of the Output Points. On status indicates that the Output Point is "on" and Off status indicates that the Output Point is "off".

Manual Actions: provide user with radio buttons selection of what manual action to perform.

The description of the second radio button is the opposite of the current status and it will toggle between On and Off.

The third radio button, *Duration On* or *Duration Off*, which is the opposite of the current status, is used to send a command to turn on or turn off the Output Point for a duration as depicted in the *Duration* field in *Output Setup* menu item.

21.1.1 To control the Output Points

1. Click on the appropriate link, 1-16 or 17-32 , to display the correct range of Output Points. Alternatively, you can click on the or button.
2. Select the desired radio button(s) (see NOTICE 1).
3. Click on either or button to send the command. The web page will refresh to reflect the new status.

NOTICE!

1. Select only Output Point(s) that you want to send command to.
2. The current status of the Output Point for a *Duration On* or *Duration Off* command will not show the true status after the *Duration* has elapsed, unless the user refreshes the web page by clicking on the button.

22 Reset APB

The Reset APB is the final menu item of the Manual Control Group. It allows user to reset the Anti-Passback (APB) feature once it is violated.

NOTICE!
This feature is applicable to Full and Soft Anti-Passback only.

If Full APB is used, this command will reset the violation and allow violator(s) to access or exit the controlled door. However, if Soft APB is used, this command will reset the Activity transactions for "Access Granted, Soft APB" and "Exit Granted, Soft APB" for violator's subsequent access or exit respectively.

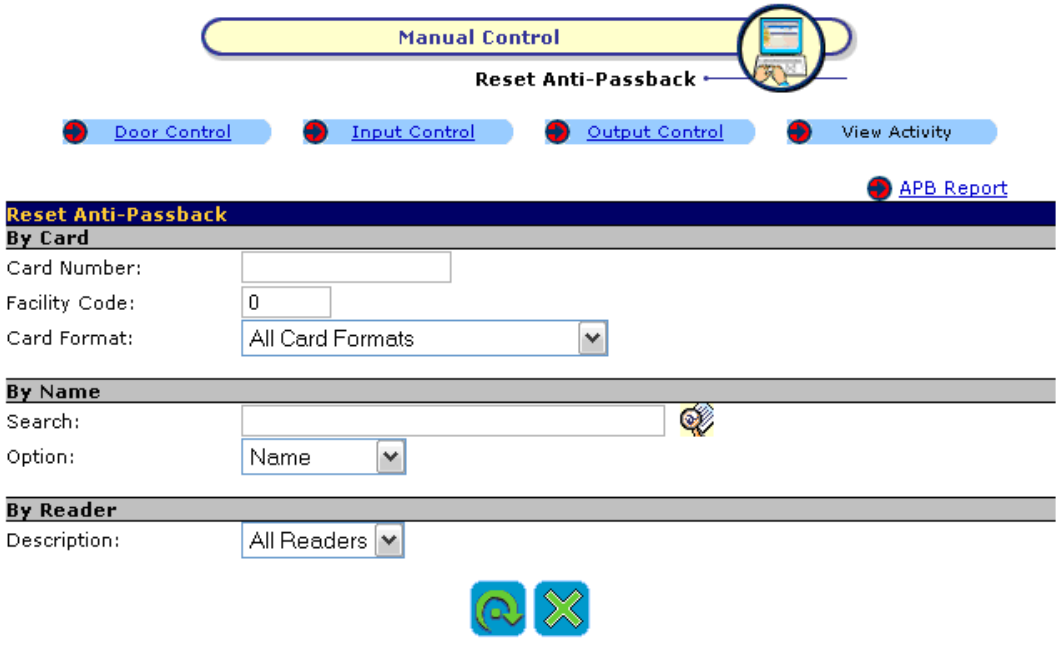
User is given the option to reset the APB violation with the following combination: -

- By Card number with respect to (wrt) Reader / All Readers, or
- By Name with respect to Reader / All Readers, or
- By All Card numbers with respect to Reader / All Readers.

22.1 To activate Reset APB

There are various ways to activate the Reset APB menu item. They are: -

1. From any menu item page, click on Reset APB hyperlink.
2. From the View Activity page, click on Reset APB hyperlink.
3. From any of the menu items page of the Manual Control Group.



22.1.1 To reset APB based on Card Number wrt Reader / All Readers

To Reset APB based on Card Number, you must know the following, Card Number, its Facility Code, and its Card Format.

1. Enter the *Card Number* of the APB violator.
2. The number in the Facility Code field is configured in *Panel Setup, Default Settings*, if the code is different from the default, then change it.
3. Select the *Card Format* from the list.
4. Select the *Reader* from the list. If you want to Reset APB wrt all readers, select *All Readers*.
5. Click on the button to proceed. If the command is executed successfully, a message indicating APB reset by card & zones with respect to reader / all readers will be displayed.
6. Click on the button to return.

22.1.2 To reset APB based on Name wrt Reader / All Readers

1. Enter a character, a portion, or the full name and click on the button. If a match is found that satisfied the entry, a window will appear with the Names. For example, enter John and click button resulted in: -

2. From the window, select the appropriate name. The selected name appears in the Name field.
3. Select the *Readers* from the list. If you want to Reset APB with respect to all readers, select *All Readers*.
4. Click on the button to proceed. If the command is executed successfully, a message indicating APB reset by name & zones with respect to reader / all readers will be displayed.
5. Click on the button to return.

22.1.3 To reset APB by All Card numbers wrt Reader / All Readers

1. Select the *Readers* from the list. If you want to Reset APB with respect to all readers, select *All Readers*.
2. Click on the button to proceed. If the command is executed successfully, a message indicating APB reset by all cards & zones with respect to reader / all readers will be displayed.
3. Click on the button to return.

22.2 To generate a Print Preview of the report

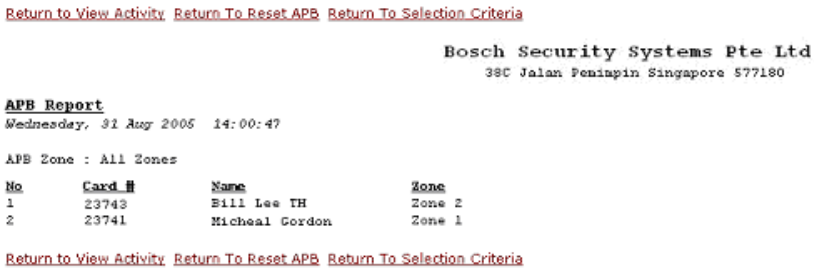
The APB Zones report allows user to know which cardholder is in the APB Zone at the time of the preview. Should there be a need to Reset APB for a particular cardholder, the user can use this report to verify that the cardholder has actually violated the APB and not due to other condition such as an Expired Card Number.

22.2.1 To generate APB Zones Report

This report shows who are the cardholders still in the APB zones. When a cardholder enter an APB zone, by opening a door from an APB entry reader, he will be registered in the system as present in the APB zone governed by the APB entry reader. Similarly, when he exit the APB zone, by opening a door from an APB exit reader, he will be de-registered in the system as been present in the APB zone governed by the APB exit reader.

1. From the first web page of the Reset APB menu item, click on the APB Zones Report link.

2. Select the desired Zone from the list.
3. Click on the button for a print preview of the report. The following screen-capture shows an example of the report.


Return to View Activity Return To Reset APB Return To Selection Criteria
Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180
APB Report
Wednesday, 31 Aug 2005 14:00:47
APB Zone : All Zones
No Card # Name Zone
1 23743 Bill Lee TH Zone 2
2 23741 Micheal Gordon Zone 1
Return to View Activity Return To Reset APB Return To Selection Criteria

If you wish to print out a hardcopy, click on the Print button located on the Toolbar of the web browser program. Alternatively, click on the *File* and select *Print*.

4. To return to the Reset APB web page, click on the Return To Reset APB link.
5. To return to the view activity page, click on the Return to View Activity link.
6. To generate a preview of other zone, click on the Return To Selection Criteria link.

23 Panel Setup

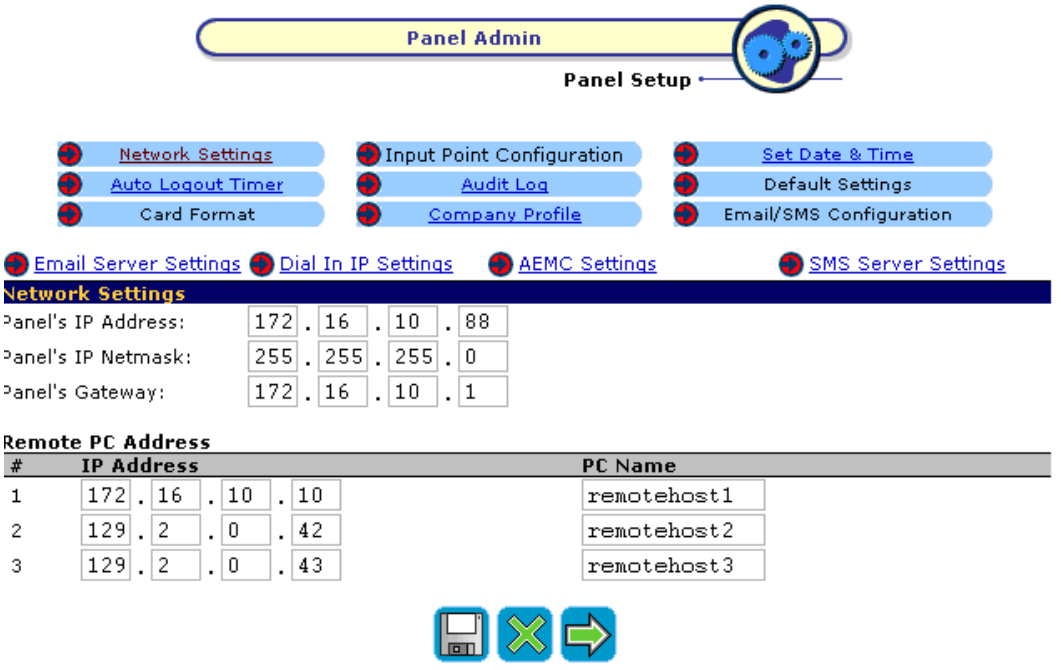
This chapter covers a step by step guide to set up the *Panel Setup*.
In the *Panel Setup*, user is allowed to set the following configuration: -

- Network Settings,
- Auto Logout Timer,
- Audit Log,
- Set Date & Time Setting,

23.1 To activate Panel Setup

The Panel Setup can be activated only from the menu item page.

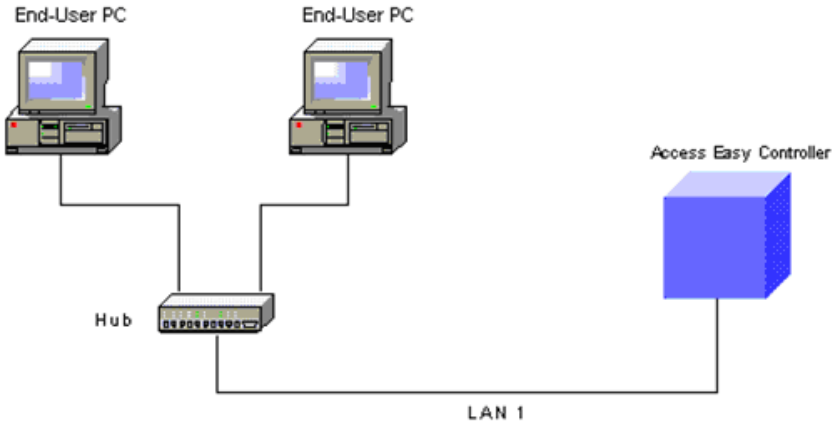
1. From any menu item page, click on Panel Setup link.


Panel Admin
Panel Setup
Network Settings
Auto Logout Timer
Card Format
Input Point Configuration
Audit Log
Company Profile
Set Date & Time
Default Settings
Email/SMS Configuration
Email Server Settings
Dial In IP Settings
AEMC Settings
SMS Server Settings
Network Settings
Panel's IP Address: 172 . 16 . 10 . 88
Panel's IP Netmask: 255 . 255 . 255 . 0
Panel's Gateway: 172 . 16 . 10 . 1
Remote PC Address
IP Address PC Name
1 172 . 16 . 10 . 10 remotehost1
2 129 . 2 . 0 . 42 remotehost2
3 129 . 2 . 0 . 43 remotehost3

23.2 Network Setting

This configuration allows user to configure the *Panel's IP, Netmask*, and *Gateway Address*. Each Access Easy Controller comes with 2 LAN ports, they are labelled as LAN1 and LAN2. These LAN ports are physically individual ports that have its own IP address.

LAN1 is connected to the network where the Access Easy Controller are accessed by other workstations, this is usually the office network. LAN2 is cater for further expansion.



In addition, user can define 3 Remote PC Addresses for ftp purposes and the address of the email server.

23.2.1 To Configure LAN 1 Network Setting

1. Click on the Network Setting to go to the Network Setting page. The IP Address setting presented is the network setting for LAN 1.
2. Highlight the default number in each of the IP Address's field and enter the appropriate number.
3. Repeat the above step for the *Panel's Netmask* and *Gateway*.
4. Click on the button (see NOTICE).

NOTICE!
In order for the new IP Address to take effect, the Controller needs rebooting.

23.3 Remote PC Addresses

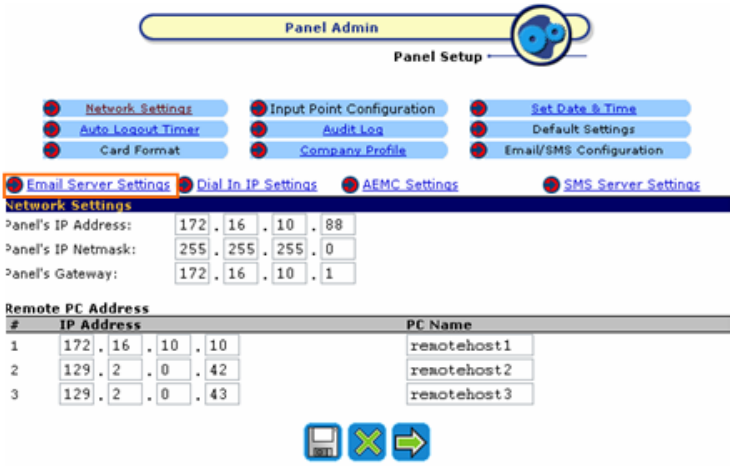
This allows user to set 3 dedicated personal computer's IP Address to allow user to down-load/upload parameters to Access Easy Controller using DB Backup utility program.

23.3.1 To edit Remote PC Addresses

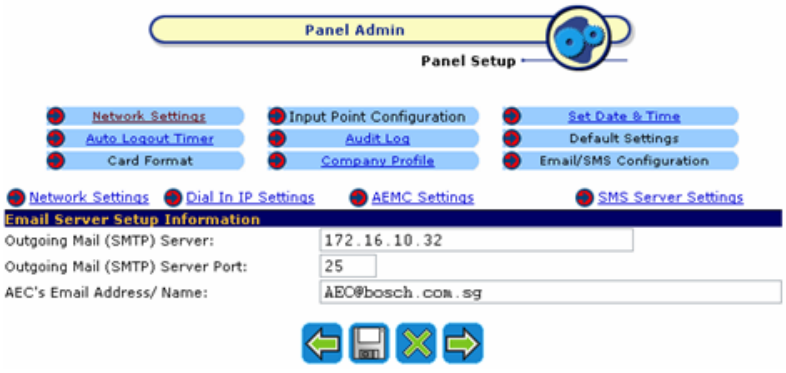
1. Highlight the default number in each of the IP Address's field and enter the appropriate number.
2. Enter the PC Name as a complete word, with no spacing in between. You can use the underscore to denote spacing.
3. Click on the button.

23.4 Email Server Setup Information

This section allows user to define the address of the Outgoing Mail (SMTP) server, the SMTP port to use and the Access Easy for Master Email Address/Name. Click on the *Email Server Setting* link to goes to the Outgoing Mail (SMTP) server configuration page.


Panel Admin
Panel Setup
Network Settings
Input Point Configuration
Set Date & Time
Auto Logout Timer
Audit Log
Default Settings
Card Format
Company Profile
Email/SMS Configuration
Email Server Settings
Dial In IP Settings
AEMC Settings
SMS Server Settings
Network Settings
Panel's IP Address: 172 . 16 . 10 . 88
Panel's IP Netmask: 255 . 255 . 255 . 0
Panel's Gateway: 172 . 16 . 10 . 1
Remote PC Address
IP Address PC Name
1 172 . 16 . 10 . 10 remotehost1
2 129 . 2 . 0 . 42 remotehost2
3 129 . 2 . 0 . 43 remotehost3

The Outgoing Mail (SMTP) Server defines the server that is to provide your email facilities and the Access Easy for Master Email Address/Name is the reply address for emails sent by the Access Easy for Master that is, the name address that is to appear in the 'sent to' field of the dispatched email.



23.4.1 To Configure the Email Server Setup Information

1. Highlight the default text in the Outgoing Mail (SMTP) Server field and enter the appropriate text.
2. The default number (25) is the commonly used port number for the Outgoing Mail (SMTP) Server, unless your configuration is different, we suggest you skip this field.
3. Enter the Access Easy for Master Address/Name as a complete word, with no spacing in between. You can use the underscore to denote spacing. The Address/Name specified in this field will be used together with the Domain name to form the email address of the Access Easy for Master. Referring to the diagram and with the Domain name "bosch.com.sg", the email address of Access Easy for Master becomes,

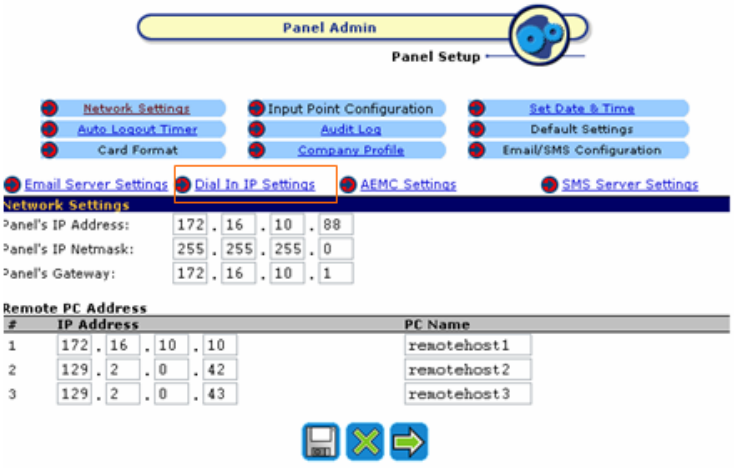
   AEC@bosch.com.sg

4. Click on the button.

23.5 Dial In IP Setup Information

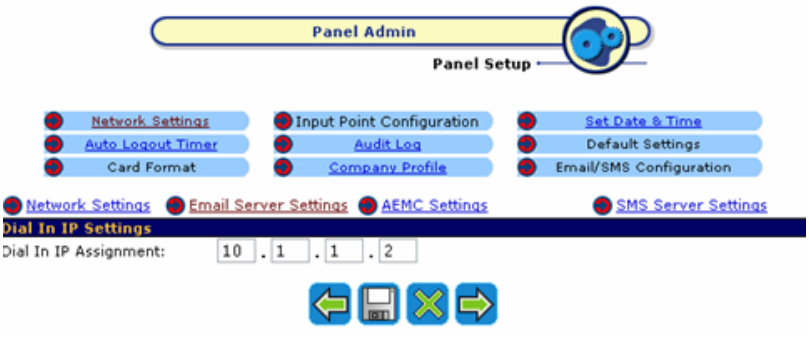
This section allows user to configure the Dial In IP that is required for PPP protocol. In order to have remote access ability using a modem for connection, a temporary IP address has to be issued to the incoming connection. When a user dialled in from home, using his PC and a modem, the Access Easy Controller's modem will answer the incoming call and negotiate with the remote modem for a suitable connection protocol and speed. If the process is successful, a temporary IP is issued to the remote modem and hence, connection is established.

By default, this *Dial in IP address* is set at 10.1.1.2. It will work fine on most network setup, however, if the user encounters connection problem, it will need to be changed. To change this setting, click on the *Dial In IP Settings* to access to the setting page.


Panel Admin
Panel Setup
Network Settings
Input Point Configuration
Set Date & Time
Auto Logout Timer
Audit Log
Default Settings
Card Format
Company Profile
Email/SMS Configuration
Email Server Settings
Dial In IP Settings
AEMC Settings
SMS Server Settings
Network Settings
Panel's IP Address: 172 . 16 . 10 . 88
Panel's IP Netmask: 255 . 255 . 255 . 0
Panel's Gateway: 172 . 16 . 10 . 1
Remote PC Address
IP Address PC Name
1 172 . 16 . 10 . 10 remotehost1
2 129 . 2 . 0 . 42 remotehost2
3 129 . 2 . 0 . 43 remotehost3

23.5.1 To edit the Dial In IP Settings Information

1. Highlight the default text in the Dial In IP Assignment fields and enter the appropriate IP address.

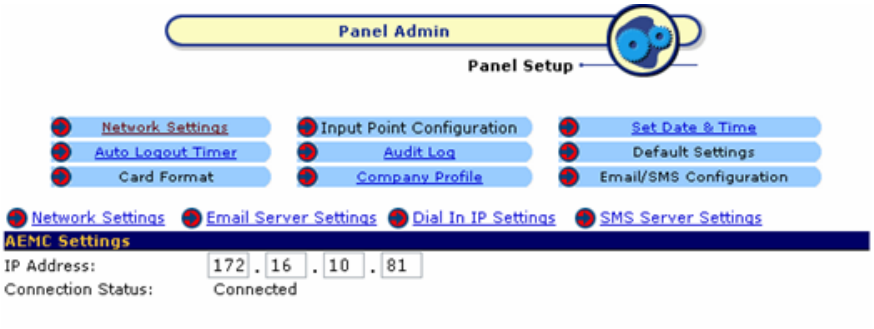


2. Click on the button

23.5.2 Access Easy Master IP Address Settings for Access Easy for Master

This section allows user to define the IP address for connection between Access Easy Master and Access Easy for Master.

1. From the *Panel Setup* screen, click on the *AEMC Settings* link.



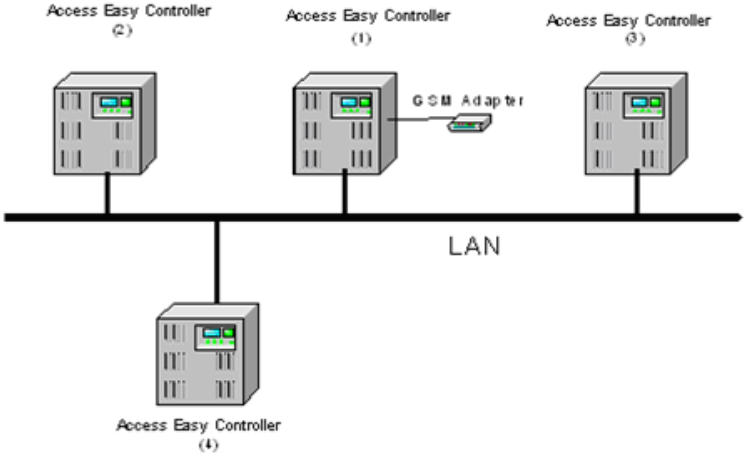
2. Enter the IP address of the Access Easy Master.

3. Click on the button or click button to save the settings.

23.5.3 SMS Server Settings Information

This section allows user to define the IP address of the Access Easy for Master that has a GSM adapter attached to its serial com acting as the SMS server. To briefly understand how the SMS feature works, we need to understand how the system should be configured.

The following diagram shows a drawing that has more than one Access easy controller in the network. These controllers work stand-alone but shared a common GSM adapter, which is attached to a dedicated access easy controller serial com port.



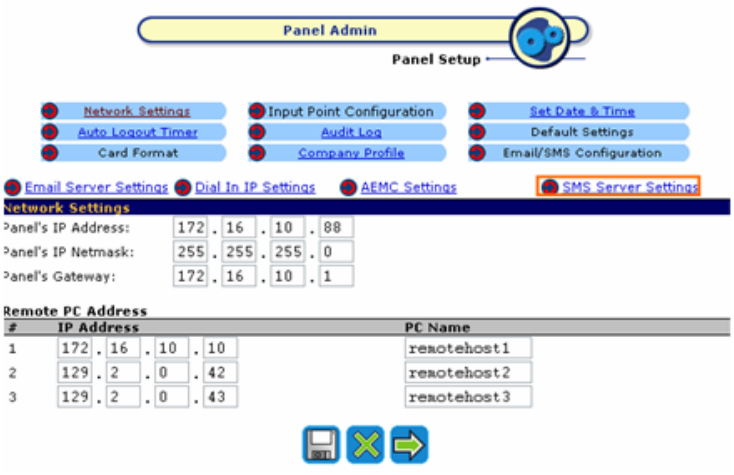
The Access Easy Controller (1) has the GSM adapter connected to it's serial com port, hence, it is also acting as a SMS Server to help relay the other Access Easy for Master messages to the Service Provider.

NOTICE!
Please ensure that GSM adapter baudrate is configure at 19200bps, 8bit data, 1 stop bit and no parity settings. Please refer to the Appendix G for details and models, adapter of GSM that support this feature.

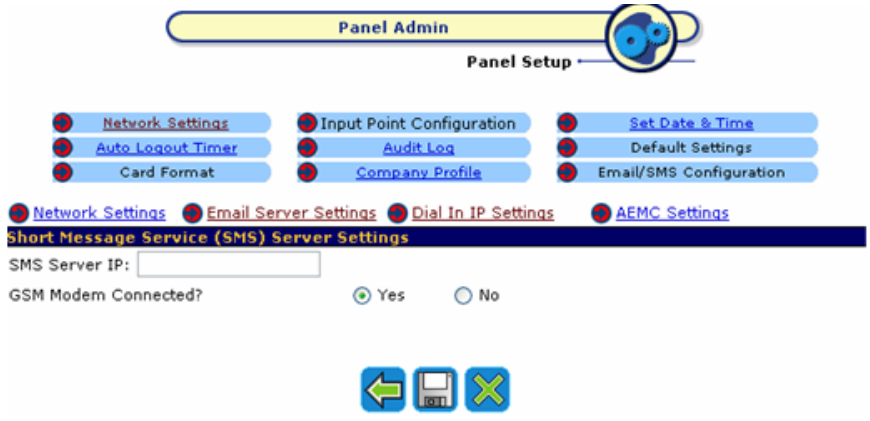
Whenever, there is any SMS message that needed to be send, the respective Access Easy for Master will send the SMS messages over to the Access Easy for Master SMS Server and the SMS Server will send via the GSM adapter to the Service Provider. These controllers are defined as the SMS Client. Hence, there is a need to control which is the IP Address that is allowed to send SMS, this is to prevent unauthorised personnel sending SMS via your Access Easy Controller.

To Configure Access Easy for Master as a SMS Server

By default, the *SMS Server IP* address is blank. If this controller is attached to a GSM adapter, you will need to configure the IP address of other Access Easy for Master that will send SMS message through it. To change this setting, click on the *SMS Server IP* Settings to access to the setting page, as shown in the following diagram.


Panel Admin
Panel Setup
Network Settings
Input Point Configuration
Set Date & Time
Auto Logout Timer
Audit Log
Default Settings
Card Format
Company Profile
Email/SMS Configuration
Email Server Settings
Dial In IP Settings
AEMC Settings
SMS Server Settings
Network Settings
Panel's IP Address: 172 . 16 . 10 . 88
Panel's IP Netmask: 255 . 255 . 255 . 0
Panel's Gateway: 172 . 16 . 10 . 1
Remote PC Address
IP Address PC Name
1 172 . 16 . 10 . 10 remotehost1
2 129 . 2 . 0 . 42 remotehost2
3 129 . 2 . 0 . 43 remotehost3

1. The SMS Server Setting page is shown below:



2. Since this is an SMS Server, we will select "Yes" for GSM Modem Connected?" and click the save button.
3. You will need to reboot the Access Easy for Master for the changes to take place.

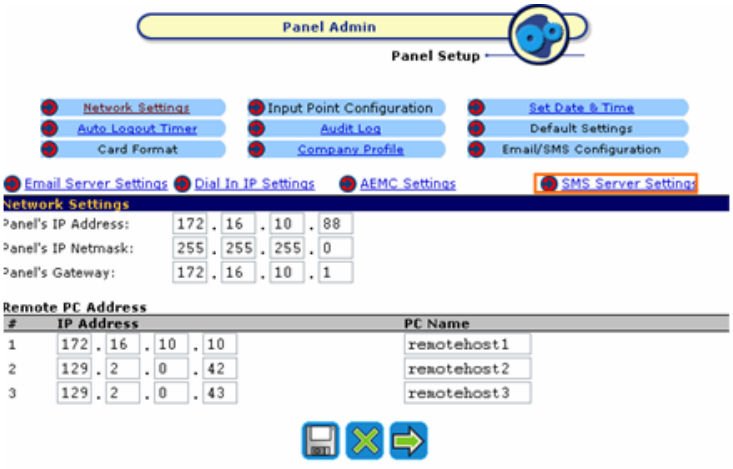
4. After rebooting, goes back to the SMS Server page and you will see the following :

5. There are up to 10 Remote Controller addresses that you could configure. These addresses are the IP Address of those access easy controllers that send SMS messages via the SMS Server, you should include the IP address of this AEC that has the GSM adapter connected to it.

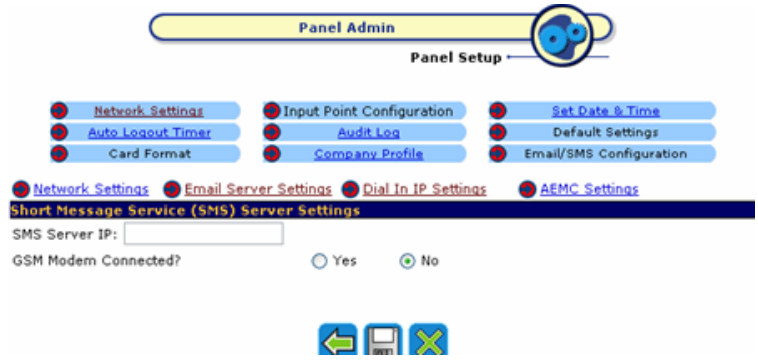
6. Click on the button to save the new settings.

To Configure Access Easy for Master as a SMS Client

By default, the *SMS Server IP* address is blank. If this controller is not attached to a GSM adapter, it is a SMS Client and hence need to identify the IP Address of the SMS Server. To change this setting, click on the *SMS Server IP Settings* to access to the setting page, as shown in the following diagram.


Panel Admin
Panel Setup
Network Settings
Input Point Configuration
Set Date & Time
Auto Logout Timer
Audit Log
Default Settings
Card Format
Company Profile
Email/SMS Configuration
Email Server Settings
Dial In IP Settings
AEMC Settings
SMS Server Settings
Network Settings
Panel's IP Address: 172 . 16 . 10 . 88
Panel's IP Netmask: 255 . 255 . 255 . 0
Panel's Gateway: 172 . 16 . 10 . 1
Remote PC Address
IP Address PC Name
1 172 . 16 . 10 . 10 remotehost1
2 129 . 2 . 0 . 42 remotehost2
3 129 . 2 . 0 . 43 remotehost3

1. The SMS Server Setting page is shown below:



2. Since this is an SMS Client, we will need to enter the IP Address of the SMS Server in the "SMS Server IP" field and click the save button.
3. You will need to reboot the Access Easy for Master for the changes to take place.

NOTICE!

Due to there is a limited number of Serial com port available in the CPU, only either the GSM adapter or the Analogue Dial-up modem can be connected to the Access easy controller, hence, dial-up features will not be enable when SMS server is be configured, like wise to the SMS server when Dial-up is been setup.

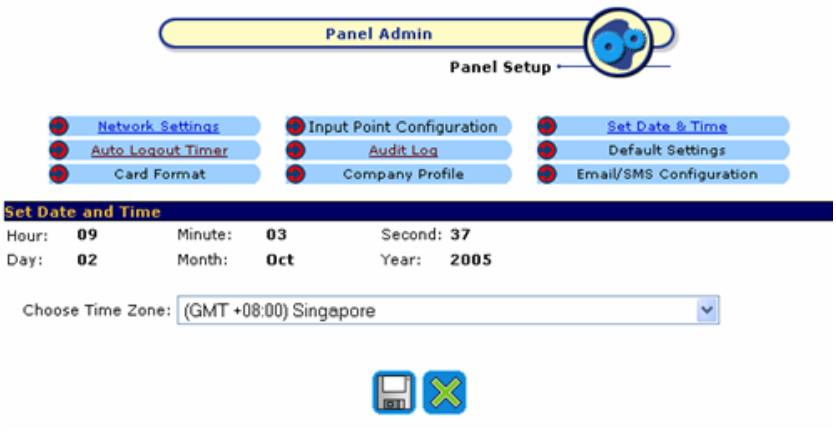
23.6 Set Date & Time

The Access Easy for Master allows user to set the *Date* and *Time* of the real-time clock within the controller. For countries that practice Daylight Saving Time, the feature is included. Time setting is in the 24-hour format.

The Date and Time set here is displayed on the status bar of the web browser during the View Activity.

23.6.1 To activate Date & Time Setting

1. From the *Panel Setup* screen, click on the *Set Date & Time* bar.



23.6.2 To set the Date & Time

1. Select your Time Zone from the list and click on the button.

NOTICE!
If your country is not listed, please select an alternative country that uses the same Time Zone.

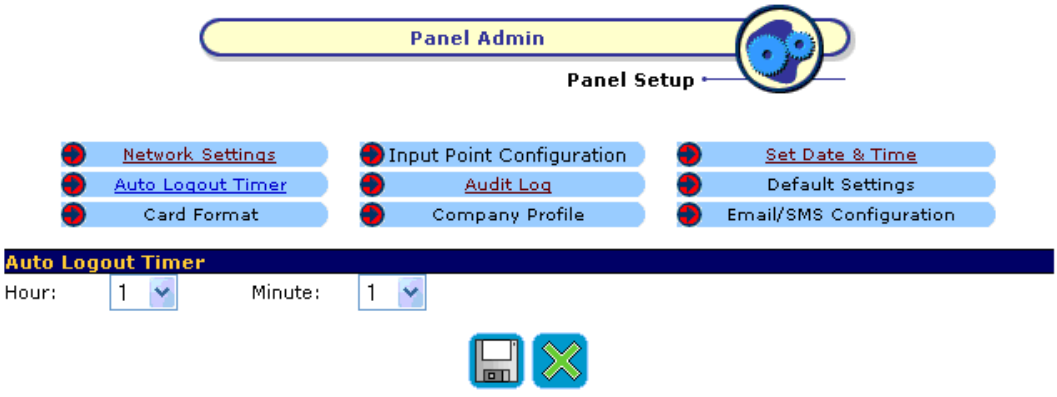
23.7 Auto Logout Timer

This configuration allows user to set the timer for the Access Easy for Master to *Logout* automatically if it detects no user activity. Default setting is 1 hour.

NOTICE!
This Timer setting is applicable to all menu items except View Activity.

23.7.1 To activate Auto Logout Timer

1. From the *Panel Setup* screen, click on the *Auto Logout Timer* link.



To edit the Auto Logout Timer

1. Select the hour and minutes from the list.
2. Click on the button.

23.8 Audit Log

The Access Easy for Master keeps 2 types of log.

- User Log
- System Log

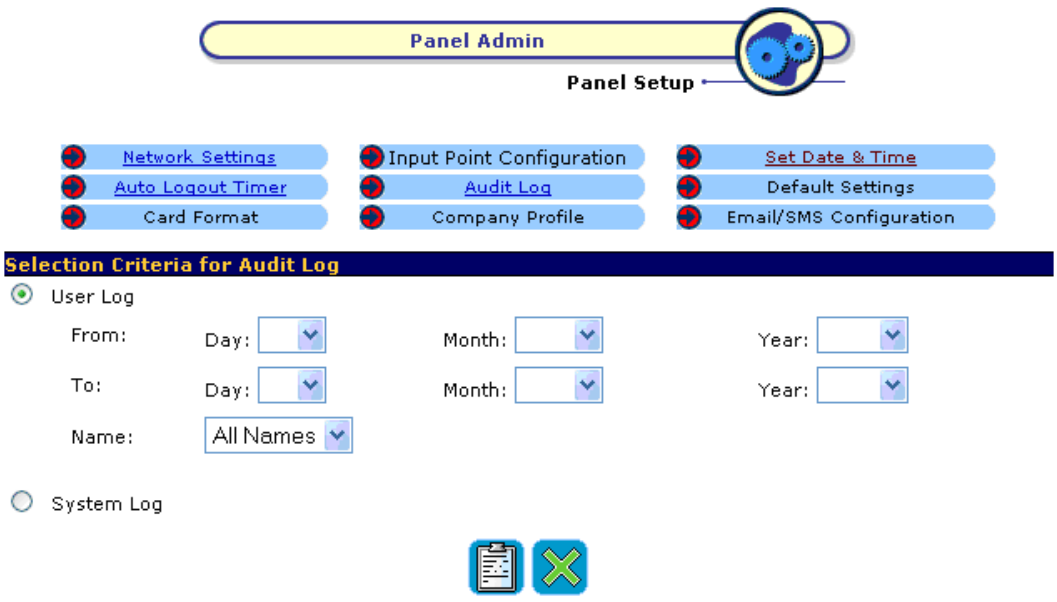
User log tracks the Users operation on the Access Easy for Master , it logs all the action performed by the user, such as manual on/off any output, change the settings for a Cardholder, set the date and time, etc.

It is a form of audit trail that could be used to keep track of what are the changes done of the system.

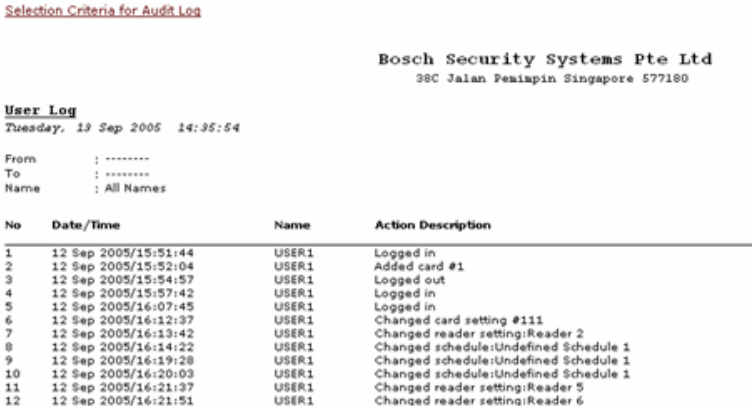
System log keep track of some of the important information of the system, such as mac address, last boot time, current boot time, version of the software, etc.

23.8.1 To View the User Log

1. Click on the *Audit Log* on any of the *Panel Setup* page and the following page will be shown.



2. Select the radio button for the User Log, as shown above.
3. Choose the From date and To date, from the pull-down list.
4. Select the User Name from the pull-down list box of the field Name. If a particular User has been selected, the report will only shows the operation of that User. If "All Names" is selected, the result will be a report containing all the action taken by all users on this system.
5. Click the button to request Access Easy for Master to enquiry for the report.
6. The following is a screen capture of how the report will looks like.



Selection Criteria for Audit Log

Bosch Security Systems Pte Ltd
38C Jalan Pemimpin Singapore 577180

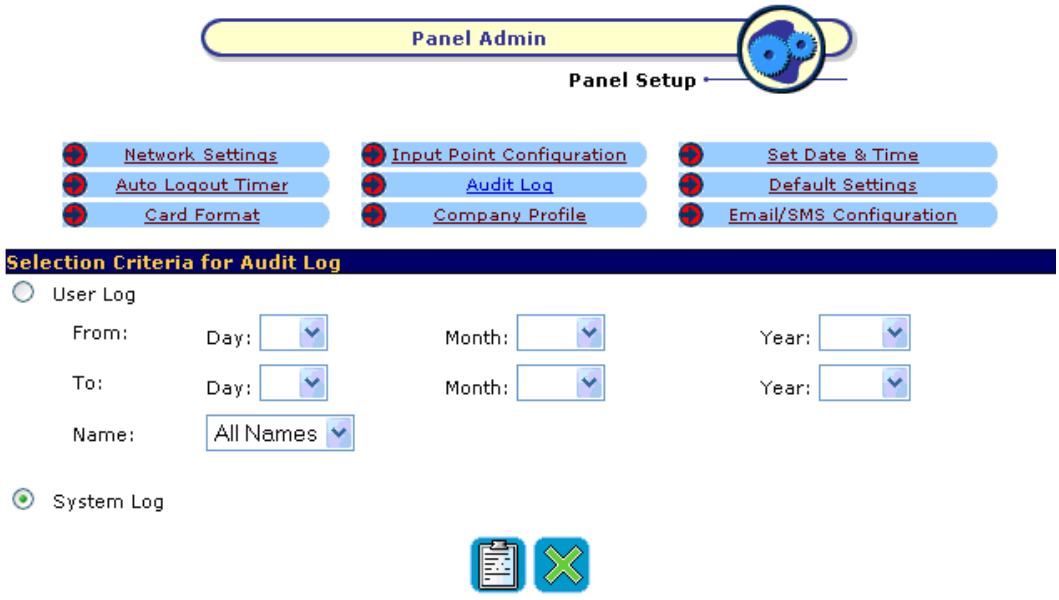
User Log
Tuesday, 13 Sep 2005 14:35:54

From : --------
To : --------
Name : All Names

No	Date/Time	Name	Action Description
1	12 Sep 2005/15:51:44	USER1	Logged in
2	12 Sep 2005/15:52:04	USER1	Added card #1
3	12 Sep 2005/15:54:57	USER1	Logged out
4	12 Sep 2005/15:57:42	USER1	Logged in
5	12 Sep 2005/16:07:45	USER1	Logged in
6	12 Sep 2005/16:12:37	USER1	Changed card setting #111
7	12 Sep 2005/16:13:42	USER1	Changed reader setting:Reader 2
8	12 Sep 2005/16:14:22	USER1	Changed schedule:Undefined Schedule 1
9	12 Sep 2005/16:19:28	USER1	Changed schedule:Undefined Schedule 1
10	12 Sep 2005/16:20:03	USER1	Changed schedule:Undefined Schedule 1
11	12 Sep 2005/16:21:37	USER1	Changed reader setting:Reader 5
12	12 Sep 2005/16:21:51	USER1	Changed reader setting:Reader 6

23.8.2 To View System Log

1. Click on the Audit Log on any of the Panel Setup page and the following page will be shown.



2. Select the radio button for the System Log, as shown above.
3. Click on the button to request Access Easy for Master to enquiry for the report.
4. The following is a sample of the System Log.

Selection Criteria for Audit Log

Bosch Security Systems Pte Ltd
38C Jalan Peminpin Singapore 577180

System Log
Friday, 23 Dec 2005 15:35:07

Product Name	:	AEC 5.6.37.27-2
Hardware Address (MAC)	:	00:04:5F:80:36:A8
Internet Address	:	172.16.10.92
Last Boot Time	:	Wed Dec 21 19:15:31 SGT 2005
Current Boot Time	:	Fri Dec 23 15:16:19 SGT 2005
Last Backup Time to Flash	:	----------
No. of Convertor/s Exist	:	2
Convertor # 1	:	Reader Ports: 01,02,03,04,05,06,07,08
	:	Reader IO: 01-08,09-16
Convertor # 3	:	Reader Ports: 09,10,11,12,13,14,15,16
	:	Reader IO: 17-24,25-32
SIM serial number	:	----------

Selection Criteria for Audit Log

The following table provides a brief explanation of the content of the System Log.

Items on the report	Explanation
Product Name	Version number of the Access Easy for Master
Hardware Address (MAC)	This is the mac address of the Access Easy controller, it is the physical address. This information could be used in the ARP command to set the IP address of the Access easy controller.
Internet Address	This is the IP address of the Access Easy for Master.
Last Boot Time	This indicates the previous time that the controller was rebooted via the Reboot link.
Current Boot Time	This indicates the most recent time that the controller was rebooted via the Reboot link. The next reboot using the Reboot link will shift this information to the Last Boot Time column.
Last Backup Time to Flash	This indicates the most recent time that the Database was backup. Database Backup could be done manually, or automatically on a daily basis.
No. of Converter/s exists	Shows how many Converter(s) card are connected to the CPU.
Converter # n ("n" denotes the address of the Converter Card)	This indicates the Readers, Input and outputs that this Converter is connected to.

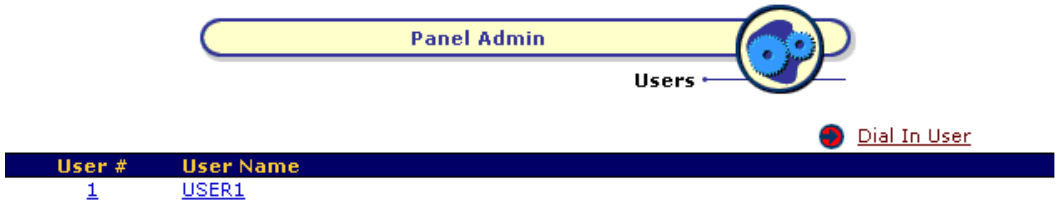
24 Users

Only one user can be assigned access rights to access and carry out the functions of the Access Easy for Master.

By default, User1 is defined as the *Super-User* having access to Access Easy for Master features.

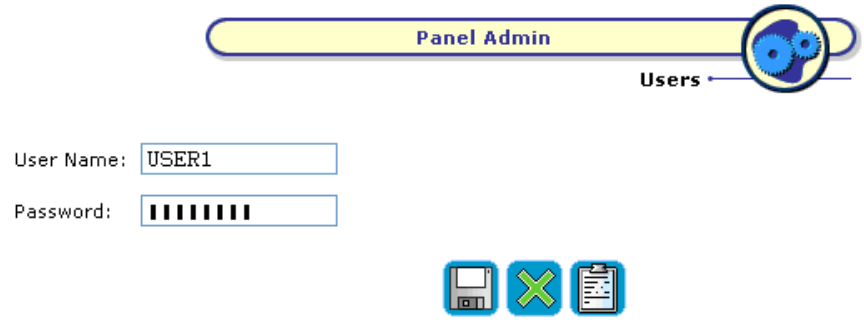
24.1 To activate Users

Since Users is the first menu item of the Panel Admin group, from the Home page, click on Panel Admin or its icon button. However, if you are in other menu item page, click directly on the Users link.



24.1.1 To edit User ID and Password

1. Click on the *numbering* or the *Description* text to proceed.



2. To edit the *User Name*, highlight the default *User Name* and enter the new *User Name*, limiting to eight alphanumerical characters including punctuation marks.
3. To edit the *Password*, highlight the default *Password* and enter the new *Password*, limiting to eight alphanumerical characters including punctuation marks (see NOTICE 1 and 2).

NOTICE!

1. The *Password* is case-sensitive.
2. For security reason, every character entered for the *Password* is represented by an asterisk. For *Macintosh* user, it is represented by a dot instead.

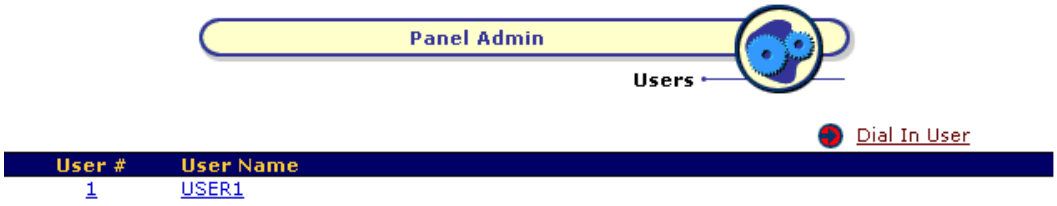
25 Dial in User

Dial-in user is a feature available in Access Easy for Master by which a user can connect to Access Easy for Master through telephone dial-in. This feature is useful when a user wants to remotely connect to his Access Easy Controller. The following steps will explain how to use this feature.

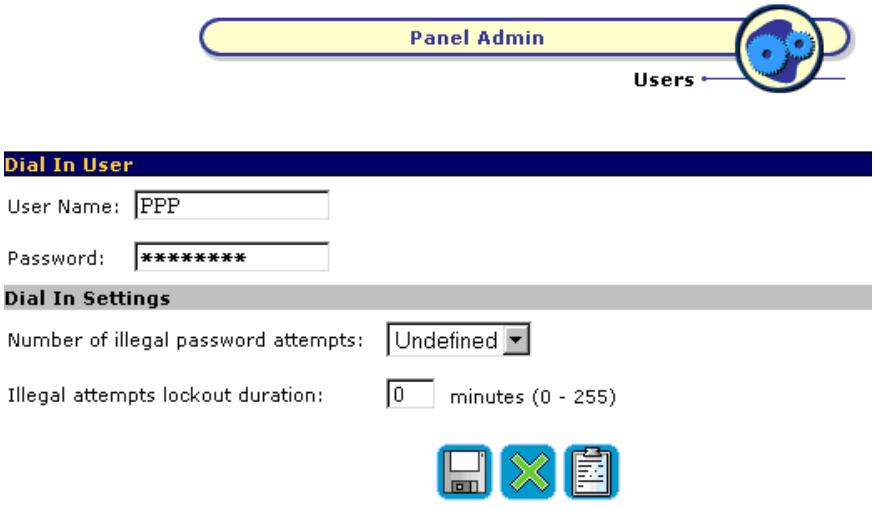
25.1 Setting up Windows for Dial-in

The steps below will explain how to make your Access Easy for Master receive a dial-in request from a PC.

1. Log on to Access Easy for Master. From any window of Access Easy for Master, click on users. You will see a screen that displays the users. On this screen, click on the dial-in user button as shown in the screen shot below.



2. Next you will come to a screen which displays the dial-in user name and password. Enter the User name and password in the appropriate boxes and click on save button indicated by floppy icon.



NOTICE!
CHANGE THE DEFAULT USER NAME AND PASSWORD AND SAVE THE NEW SETTINGS BY CLICKING ON SAVE BUTTON INDICATED BY FLOPPY ICON

3. The default user name and password has to be changed for security reasons. Enter the changed user name and password. You may also set the number of illegal password attempts and the illegal attempts lockout duration as shown in the screen.

4. The Number of illegal password attempts drop down box allows you to set the number of times the system will let you enter an illegal password before locking you out.

5. The Illegal attempts lockout duration box allows you to set the duration to disable the dial-in feature after a number of illegal password attempts as specified in step 4.

6. Click Save button to save configuration.

7. Make sure that a 56K modem is connected to your Access Easy Controller and is powered up. The modem must be connected to your telephone line to receive a dial-in request. Access Easy for Master will initialise the modem when it is re-booted.

8. Re-boot the Access Easy for Master.

9. Now your Access Easy for Master is ready to receive a dial-in request.

NOTICE!

1. The modem has to be power up and connected to the Access Easy Controller before the Access Easy Controller reboots. Access Easy Controller will initialise the modem to auto answer mode .If initialising is not done, dial-in will not be successful.

2. Once initialised, the modem will always go into auto answer mode when power up.

The following setup will guide you through the settings that are needed on your PC in order to dial into the Access Easy for Master.

1. Firstly, you will need to change the IP address of your PC which you intend to use to connect to Access Easy for Master via modem to a different network segment.

For example : the Access Easy for Master having a IP address of 129.2.0.41 and the subnetmask is 255.255.255.0, the dial-in PC could have any IP address but the subnetmask must not be 255.255.255.0, it could be 255.255.0.0 or 255.0.0.0

After changing the IP address of your dial-in PC, remember to reboot the PC before proceeding to the next step.

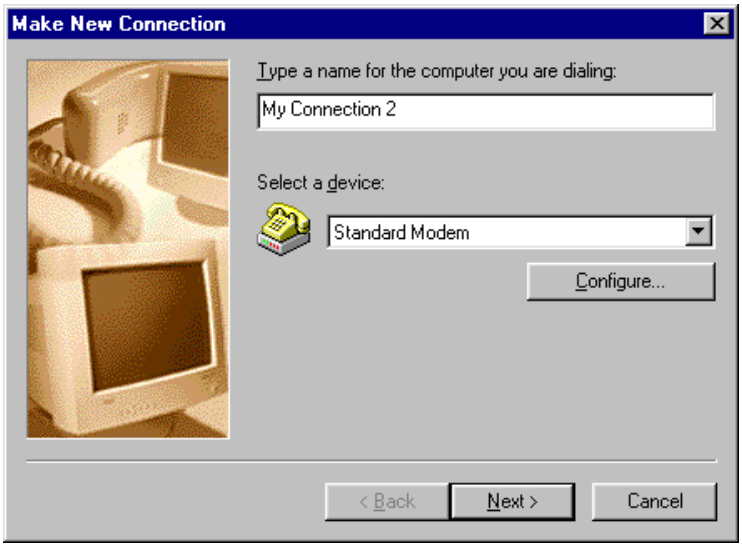
2. Now you will need to setup the dial-in connection. Click on Start button. Select Programs-Accessories-Communications- Dial-up networking as shown below and click on Dial-Up Networking.

3. You will be led to a screen as shown below.

Dial-Up Networking
File Edit View Go Favorites Connections Help
Back Forward Up Map Drive Disconnect
Address Dial-Up Networking
Make New Connection

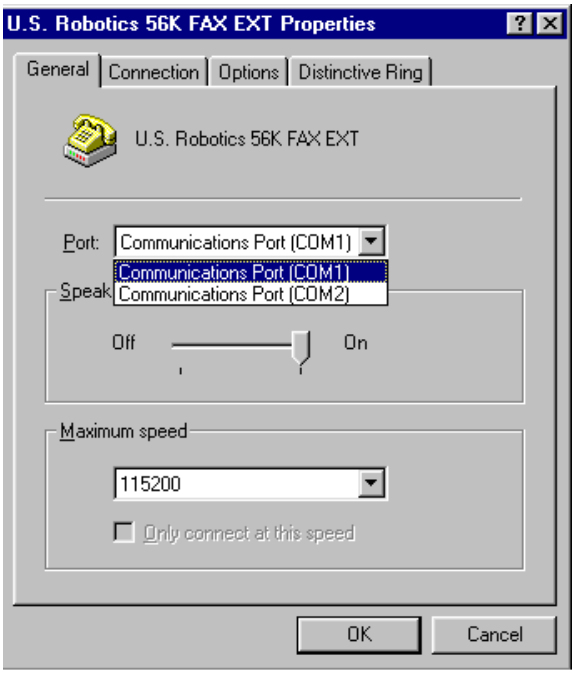
Double click on the Make New Connection icon to make a new connection.

4. You will be led to a screen as shown below.

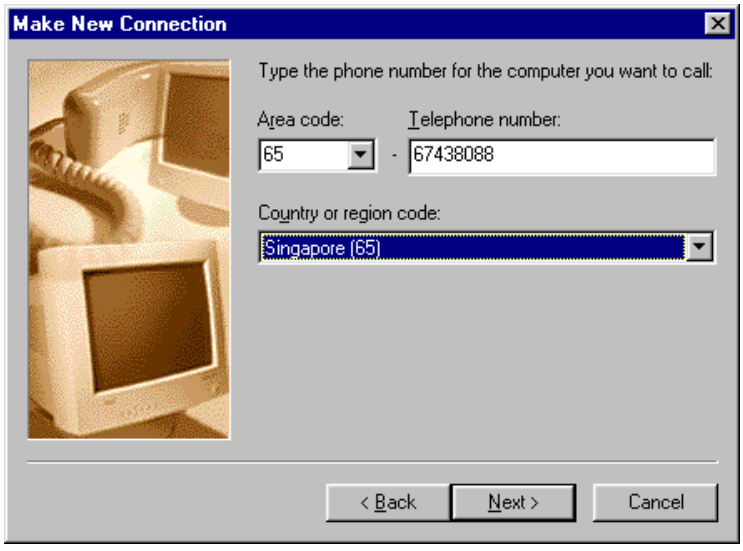


5. Follow the instructions on the screen. Make sure that a modem is connected to your PC. Select the appropriate modem by clicking on the Select a device drop down box.

6. Next, configure your modem by clicking on the configure button and entering the various configuration options as shown in the next screen shot.

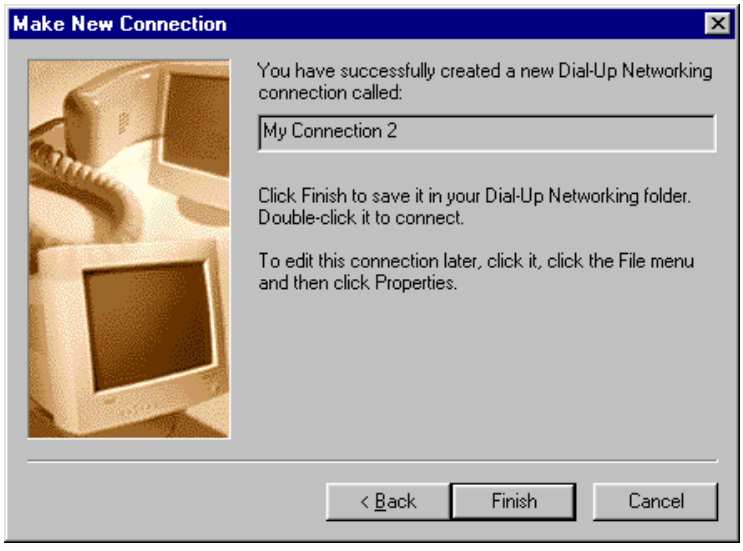


7. After configuring your modem, click on next and you will see a screen as shown in the next screen shot.



Enter the telephone number for the Access Easy for Master that you want to connect to and click on next.

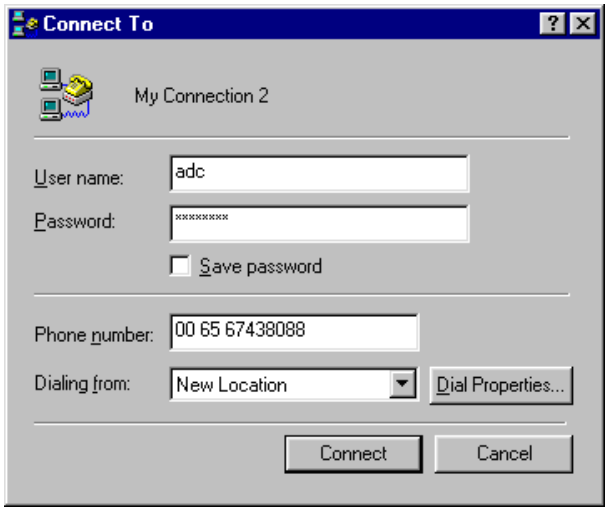
8. You will see a screen as shown below.


Make New Connection
You have successfully created a new Dial-Up Networking connection called:
My Connection 2
Click Finish to save it in your Dial-Up Networking folder. Double-click it to connect.
To edit this connection later, click it, click the File menu and then click Properties.
< Back
Finish
Cancel

Click on *Finish* to complete your connection.

9. After clicking on Finish you would have created a new connection named 'My Connection 2' as shown below

10. To Connect to the Access Easy for Master, double click on My Connection and you will be led to a screen as shown below.



In the User name and Password box, enter the Dial-In User name and Password of the Access Easy for Master which you want to connect to. In the phone number box, enter the phone number for the Access Easy for Master you want to connect to and then click on the Connect button.

11. After successfully connecting, you have to log on to the Access Easy for Master as shown in the screenshot below from the Web Browser application.
12. Enter the User ID and Password of the Access Easy for Master in the appropriate fields.

NOTICE!
Do NOT enter the Dial-In User Name and Password, it should be the normal login User ID and Password that you use to login the Access Easy for Master in a LAN environment.

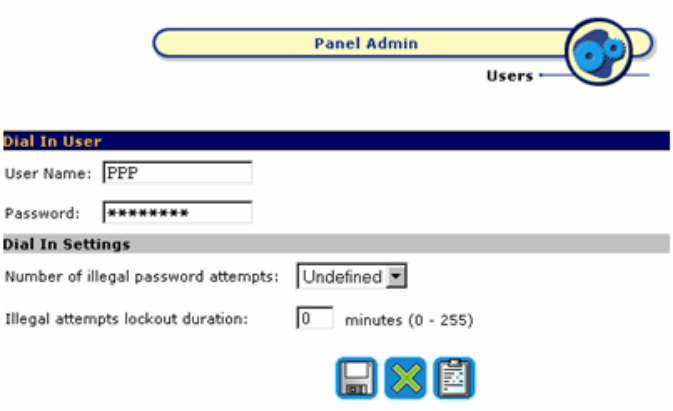
13. After successful log in to the Access Easy for Master, you can now proceed with the normal operation as if you are in the office.

25.2 Setting up Macintosh for Dial-in

The above steps pertain to PC. For Mac OS, please follow the steps as explained.

1. Log on to Access Easy for Master. From any window of Access Easy for Master, click on users. You will see a screen that displays the users. On this screen, click on the dial-in user button as shown in the screen shot below.

2. Next you will come to a screen which displays the dial-in user name and password. Enter the User name and password in the appropriate boxes..



NOTICE!
CHANGE THE DEFAULT USER NAME AND PASSWORD AND SAVE THE NEW SETTINGS BY CLICKING ON SAVE BUTTON INDICATED BY FLOPPY ICON

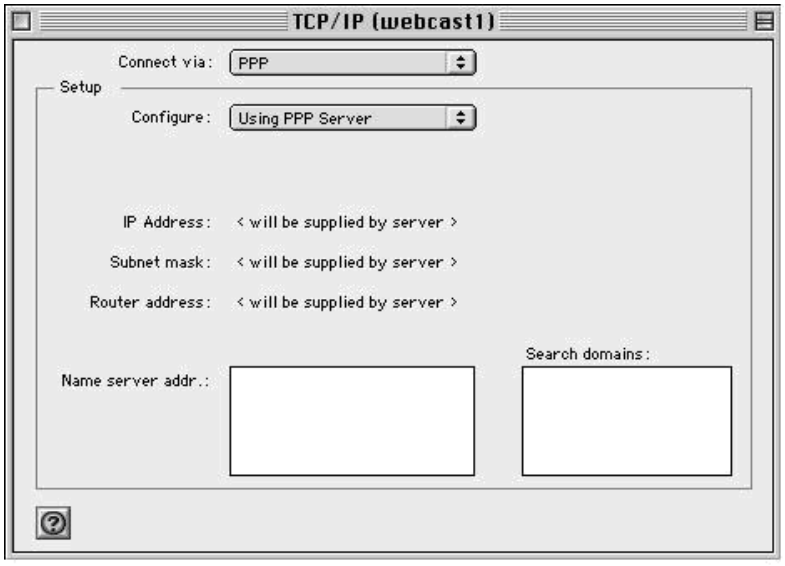
3. The default user name and password has to be changed for security reasons. Enter the changed user name and password. You may also set the number of illegal password attempts and the illegal attempts lockout duration as shown in the screen.
4. The Number of illegal password attempts drop down box allows you to set the number of times the system will let you enter an illegal password before locking you out.
5. The Illegal attempts lockout duration box allows you to set the duration to disable the dial-in feature after a number of illegal password attempts as specified in step 3.
6. Next, click the save button to confirm the changes and backup the Database now.
7. Make sure that a 56K modem is connected to your Access Easy Controller and is powered up. The modem must be connected to your telephone line to receive a dial-in request. Access Easy for Master will initialise the modem when it is re-booted.
8. Re-boot the Access Easy for Master.
9. Now your Access Easy for Master is ready to receive a dial-in request.

NOTICE!
1. The modem has to be power up and connected to the Access Easy Controller before the Access Easy Controller reboots. Access Easy Controller will initialise the modem to auto answer mode .If initialising is not done, dial-in will not be successful.
2. Once initialised, the modem will always go into auto answer mode when power up.

The following setup will guide you through the settings that are needed on your Mac in order to dial into the Access Easy for Master.

1. Firstly, you will need to change the IP address of your Mac which you intend to use to connect to Access Easy for Master via modem to a different network segment.For example : the Access Easy for Master having a IP address of 129.2.0.41 and the subnetmask is 255.255.255.0, the dial-in Mac could have any IP address but the subnetmask must not be 255.255.255.0, it could be 255.255.0.0 or 255.0.0.0
2. After changing the IP address of your dial-in Mac, remember to reboot the Mac before proceeding to the next step
3. Select Control Panels from the apple menu and from the Control Panels sub-menu select TCP/IP. Refer screenshot below.

4. You will be led to a screen as shown below. Change the connection settings to PPP.



5. Next, select Remote Access from the Control Panels sub-menu

6. You will be led to a screen as shown in the following. Enter the user name and password for the Access Easy for Master, which you want to connect to. Also enter the dial-in number in the Number box. Click on Connect button to remotely access the Access Easy for Master.

7. After successfully connecting to Access Easy for Master remotely, you may log on to Access Easy for Master from any browser by supplying the IP address for the Access Easy for Master and the correct Access Easy for Master user name and password.

NOTICE!
Do NOT enter the Dial-In User Name and Password, it should be the normal login User ID and Password that you use to login the Access Easy for Master in a LAN environment.

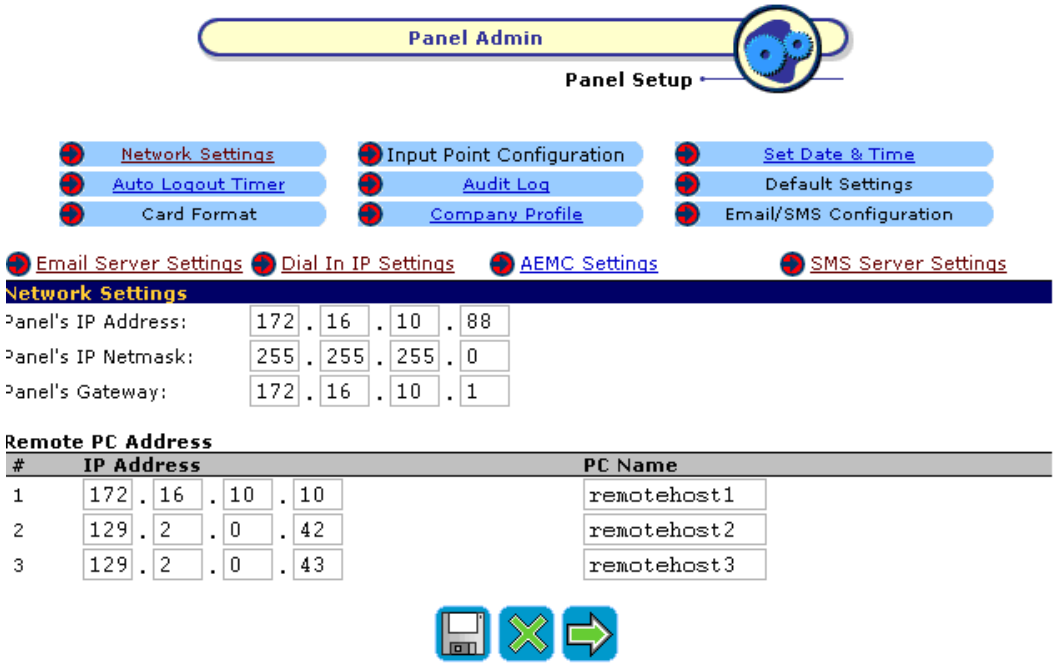
8. After successful log in to the Access Easy for Master, you can now proceed with the normal operation as if you are in the office.

26 Update Flash

This function allows Access Easy for Master parameters update to the flash to be carried out merely by a few clicks of the mouse button. User can easily use a simple ftp program (using third party program) to transfer file(s) either from *Bosch Security Systems web site* or *BOSCH SECURITY SYSTEMS dealers* to a designated location in Access Easy for Master directory, initiate the *Update Flash* and allow the Access Easy for Master software to install the program / update the flash automatically.

NOTICE!

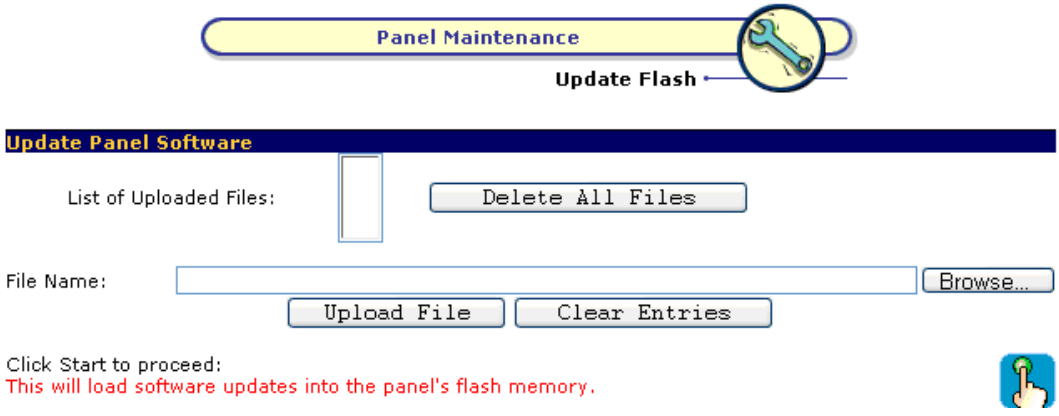
1. Please check with BOSCH SECURITY SYSTEMS or its authorised dealers for the upgrade.
2. Before attempting to ftp to the Access Easy for Master, the Remote PC IP needs to be configured first in the Panel Setup, else the panel will not allows connection. Goes to the Panel Setup of the Access Easy for Master and configure into any of the 3 remote PC setting, the PC's IP address that you intend to use for.


Panel Admin
Panel Setup
Network Settings
Input Point Configuration
Set Date & Time
Auto Logout Timer
Audit Log
Default Settings
Card Format
Company Profile
Email/SMS Configuration
Email Server Settings
Dial In IP Settings
AEMC Settings
SMS Server Settings
Network Settings
Panel's IP Address: 172 . 16 . 10 . 88
Panel's IP Netmask: 255 . 255 . 255 . 0
Panel's Gateway: 172 . 16 . 10 . 1
Remote PC Address
IP Address PC Name
1 172 . 16 . 10 . 10 remotehost1
2 129 . 2 . 0 . 42 remotehost2
3 129 . 2 . 0 . 43 remotehost3

File(s) for upgrading can be categorised as program enhancement, bugs fixing, new features... etc. For the flash update, this is usually carried out when the Access Easy Controller's CPU Card flash memories become corrupted or that the CPU Card is out of service and needed replacement to resume normal operation.
This function will permanently overwrite your existing data in the flash memories.

26.1 To activate Update Flash

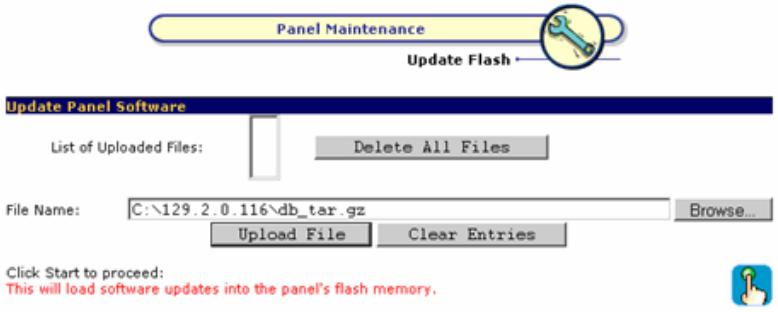
Since Update Flash is the first menu item of the Panel Maintenance group, from the Home page, click on Panel Maintenance or its icon button. However, if you are in other menu item page, click directly on the Update Flash link.



NOTICE!
The uploading of db_tar.gz will replace all configurations except IP address. This action is irreversible.

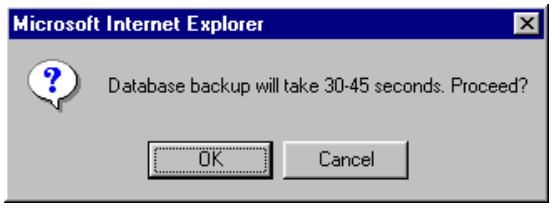
26.1.1 To Update Panel Software

1. Click on Browse... button to select the file you wish to upload. example, if you are uploading the backup system database, select the db_tar.gz from your local director



2. Click on Upload File button to upload.

3. Once the file appears in the "List of Uploaded Files, you could now click on the icon to start the updating process. The following dialog box will appear for confirmation.



4. Click on the OK button to proceed.
5. Once the process is completed without error, the following message will appear.

Upgrade Operation Completed. You need to reboot the system for the changes to take effect.

Back

6. Click on the button and reboot the Access Easy for Master.

27 Reboot Panel

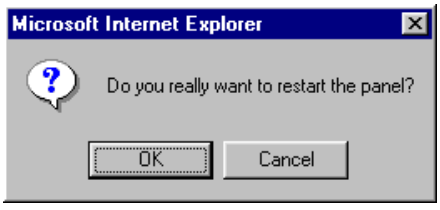
Since the Access Easy for Master's software is residing within its hardware. The Reboot Panel menu item allows user to reboot the controller after upgrading to the system software is completed or in order to allow changes made to take effect, especially changes made to Network Setting, Panel's IP Address.

CAUTION!
During a Reboot Panel function, all settings and parameters are taken from the flash memories. In such a case, it is important that the Database Backup function is carried out before proceeding to reboot the Access Easy for Master.

27.1 To activate Reboot Panel

The *Reboot Panel* can be activated only from the menu item page.

1. From any menu item page, click on the Reboot Panel hyperlink. The following dialog box appears for confirmation.



2. Click on the OK button to proceed.
3. It takes about two minutes for the process to complete (see NOTICE).

NOTICE!
During the rebooting process, the Access Easy for Master disconnect itself from the computer and the web page on the computer screen might show an error message or be completely blank. User(s) must close and re-launch the web browser program. Login to Access Easy for Master again after the process is completed.

4. Once the Access Easy for Master is up and running again, please re-enter the Access Easy for Master URL Address and proceed with the Login.

28 APPENDIX A Selecting Events, Devices and Cardholders for Reports

	Devices							Cardholders	
Events	**All Readers, Inputs and Output Point**	**All Readers**	**Selected/Omit Readers**	**All Input Points**	**Selected/Omit Input Points**	**All Output Points**	**Selected/Omit Output Points**	**All Cardholders**	**Selected/Omit Cardholders**
Panel Tamper	x	x	x	x	x	x	x	x	
Tamper Restored	x	x	x	x	x	x	x	x	
Panel AC Failure	x	x	x	x	x	x	x	x	
Power Restored	x	x	x	x	x	x	x	x	
Alarm	x			x	x			x	
Alarm Restored	x			x	x			x	
Door Forced Open	x	x	x					x	
Door Held Open	x	x	x					x	
Door Closed	x	x	x					x	
Duress	x	x	x					x	x
Access Denied	x	x	x					x	x
Access Denied - Passback	x	x	x					x	x
Exit Denied - Passback	x	x	x					x	x
Access Denied - Timed APB	x	x	x					x	x
Access Denied - Wrong PIN	x	x	x					x	x
Invalid Schedule	x	x	x					x	x
Invalid Card	x	x	x					x	
Invalid start Date	x	x	x					x	x
Invalid End Date	x	x	x					x	x
Armed	x	x	x	x	x			x	x
Disarmed	x	x	x	x	x			x	x
Armed By schedule	x			x	x			x	
Disarmed By Schedule	x			x	x			x	
Bypassed	x			x	x			x	
Access Granted	x	x	x					x	x
Exit Granted	x	x	x					x	x
Access Granted - Soft APB	x	x	x					x	x
Exit Granted - Soft APB	x	x	x					x	x
PIN Changed	x	x	x					x	x

	Devices							Cardholders	
Events	**All Readers, Inputs and Output Point**	**All Readers**	**Selected/Omit Readers**	**All Input Points**	**Selected/Omit Input Points**	**All Output Points**	**Selected/Omit Output Points**	**All Cardholders**	**Selected/Omit Cardholders**
Door Access Enabled	x	x	x					x	
Door Access Disabled	x	x	x					x	
Door Locked	x	x	x					x	
Door Unlocked	x	x	x					x	
Door Momentarily Unlocked	x	x	x					x	
Door Locked By Schedule	x	x	x					x	
Door Unlocked By Schedule	x	x	x					x	
Turned On	x					x	x	x	
Turned Off	x					x	x	x	
Duration On	x					x	x	x	
Duration Off	x					x	x	x	
Turned On By Schedule	x					x	x	x	
Turned Off By Schedule	x					x	x	x	
Clock In	x	x	x					x	x
Clock Out	x	x	x					x	x

29 APPENDIX B Configuring Alarm Events

	Devices							Cardholders	
Events	**All Readers, Inputs and Output Point**	**All Readers**	**Selected/Omit Readers**	**All Input Points**	**Selected/Omit Input Points**	**All Output Points**	**Selected/Omit Output Points**	**All Cardholders**	**Selected/Omit Cardholders**
Panel Tamper	x	x	x	x	x	x	x	x	
Panel AC Failure	x	x	x	x	x	x	x	x	
Alarm	x			x	x			x	
Door Forced Open	x	x	x					x	
Duress	x	x	x					x	x
Access Denied	x	x	x					x	x
Access Denied - Passback	x	x	x					x	x
Access Denied - Timed APB	x	x	x					x	x
Access Denied - Wrong PIN	x	x	x					x	x
Invalid Card	x	x	x					x	
Invalid End Date	x	x	x					x	x
Exit Denied - Passback	x	x	x					x	x
Invalid Schedule	x	x	x					x	x
Invalid Start Date	x	x	x					x	x

30 APPENDIX C Activity Transactions

This appendix list the various Activity transactions found within each category.

30.1 Alarm Activity

No	Transactions
1	Access Denied
2	Invalid Schedule
3	Invalid Start Date
4	Invalid End Date
5	Duress
6	Access Denied - Wrong PIN
7	Access Denied - Passback
8	Access Denied - Timed APB
9	Exit Denied - Passback
10	Invalid Card
11	Door Forced Opened
12	Door Held Open
13	Panel Tamper
14	Panel AC Failure
15	Alarm

30.2 Restore Activity

No	Transactions
1	Door Closed
2	Tamper Restored
3	Alarm Restored
4	Power Restored

30.3 Valid Activity

No	Transactions
1	Access Granted
2	Exit Granted
3	Access Granted, Soft APB
4	Exit Granted, Soft APB
5	PIN Changed
6	Disarmed
7	Armed
8	Turn On
9	Turn Off
10	Door Locked
11	Door Unlocked
12	Door Locked By Schedule
13	Door Unlocked By Schedule
14	Door Momentarily Unlocked
15	Door Access Enabled
16	Door Access Disabled
17	Armed By Schedule
18	Disarmed By Schedule
19	Bypassed
20	Turned Off By Schedule
21	Turned On By Schedule
22	Duration Off
23	Duration On

30.4 Time Attendance

No	Transactions
1	Clock In
2	Clock Out

31 APPENDIX D Email/SMS Configuration Table

This Appendix provides information on how to select the appropriate item options with reference to the Events list. For each Event, an "X" indicates the possible selection that can be made under the Devices and Cardholders column.

For example, in order for Access Easy Controller to send an Email or SMS when an "Alarm" or "Alarm Restored" occurs on Input 1. The following must be set :

Devices :
"Selected Device Only option" and choose only Input 1.

Events :
"Selected events only" option and choose "Alarm" and "Alarm Restored"

Cardholders
"All Cardholders"

For this scenario, never choose "Selected Cardholders only" for Cardholders settings or "Selected Readers" or "All Readers" for Devices setting, these settings will result in not receiving any events that will meet the criteria. Cause the events for "Alarm" and "Alarm Restored" will never comes with a cardholder's ID and it will never happens on a reader.

	Devices							Cardholders	
Events	**All Readers, Inputs and Output Point**	**All Readers**	**Selected/Omit Readers**	**All Input Points**	**Selected/Omit Input Points**	**All Output Points**	**Selected/Omit Output Points**	**All Cardholders**	**Selected/Omit Cardholders**
Panel Tamper	x	x	x	x	x	x	x	x	
Tamper Restored	x	x	x	x	x	x	x	x	
Panel AC Failure	x	x	x	x	x	x	x	x	
Power Restored	x	x	x	x	x	x	x	x	
Alarm	x			x	x			x	
Alarm Restored	x			x	x			x	
Door Forced Open	x	x	x					x	
Door Held Open	x	x	x					x	
Door Closed	x	x	x					x	
Duress	x	x	x					x	x
Access Denied	x	x	x					x	x
Access Denied - Passback	x	x	x					x	x
Exit Denied - Passback	x	x	x					x	x
Access Denied - Timed APB	x	x	x					x	x
Access Denied - Wrong PIN	x	x	x					x	x
Invalid Schedule	x	x	x					x	x
Invalid Card	x	x	x					x	
Invalid start Date	x	x	x					x	x
Invalid End Date	x	x	x					x	x
Armed	x	x	x	x	x			x	x
Disarmed	x	x	x	x	x			x	x
Armed By schedule	x			x	x			x	
Disarmed By Schedule	x			x	x			x	
Bypassed	x			x	x			x	
Access Granted	x	x	x					x	x
Exit Granted	x	x	x					x	x
Access Granted - Soft APB	x	x	x					x	x
Exit Granted - Soft APB	x	x	x					x	x
PIN Changed	x	x	x					x	x
Door Access Enabled	x	x	x					x	
Door Access Disabled	x	x	x					x	

	Devices							Cardholders	
Events	**All Readers, Inputs and Output Point**	**All Readers**	**Selected/Omit Readers**	**All Input Points**	**Selected/Omit Input Points**	**All Output Points**	**Selected/Omit Output Points**	**All Cardholders**	**Selected/Omit Cardholders**
Door Locked	x	x	x					x	
Door Unlocked	x	x	x					x	
Door Momentarily Unlocked	x	x	x					x	
Door Locked By Schedule	x	x	x					x	
Door Unlocked By Schedule	x	x	x					x	
Turned On	x					x	x	x	
Turned Off	x					x	x	x	
Duration On	x					x	x	x	
Duration Off	x					x	x	x	
Turned On By Schedule	x					x	x	x	
Turned Off By Schedule	x					x	x	x	
Clock In	x	x	x					x	x
Clock Out	x	x	x					x	x

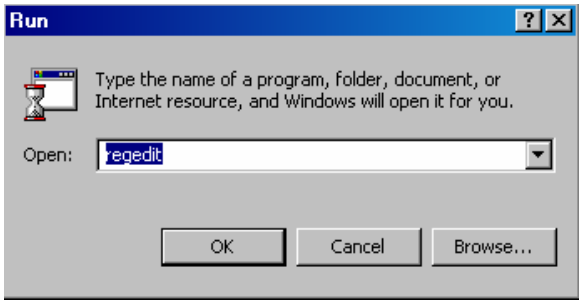
32 APPENDIX E Setting up a Timeserver

This Appendix provides information on how to set up a timeserver on windows 2000, XP Pro PC. The following section uses Windows 2000 and XP Pro to illustrate how the timeserver is set up.

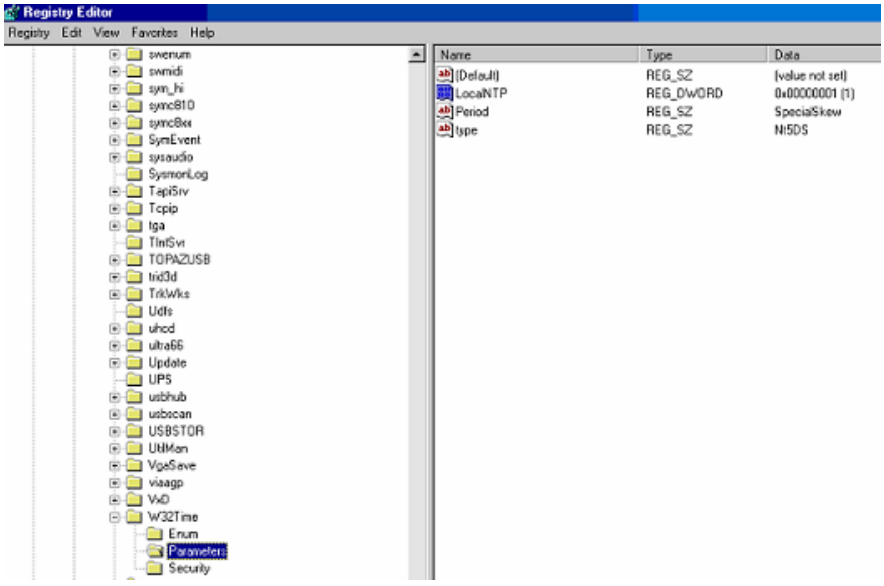
32.1 For Windows 2000

1. Click

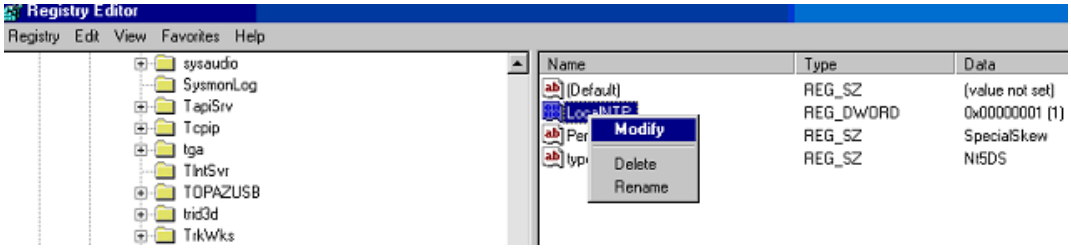
Start button and select *Run* button.
2. Type *regedit* in the window.



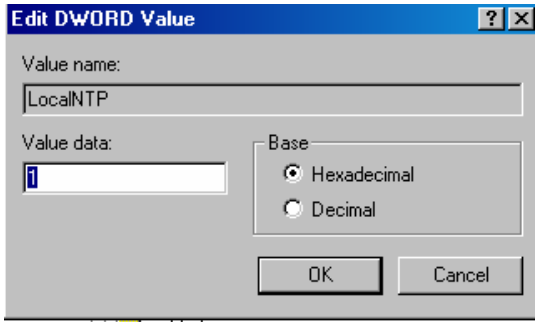
3. Select HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/SERVICES/W32TIME/PARAMETERS.



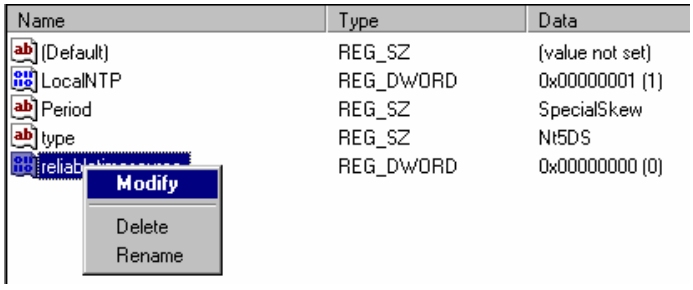
4. Right click *LocalNTP* and select *Modify*.



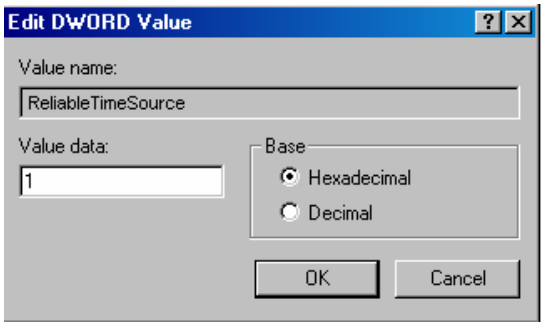
5. Enter 1 for *Value data* and click *OK*.



6. Right click *ReliableTimeSource* and select *Modify*.



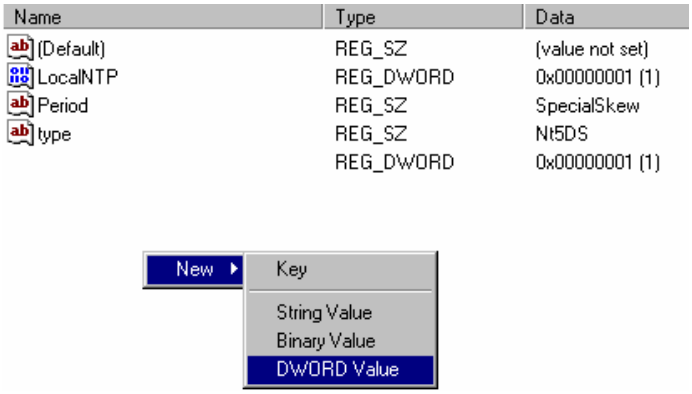
7. Enter 1 for *Value data* and click *OK*.



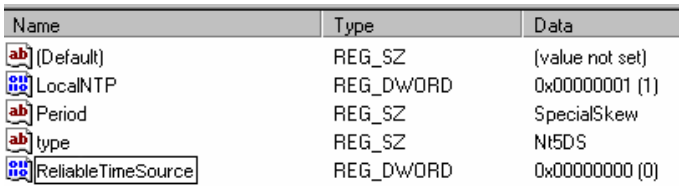
NOTICE!

If HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/SERVICES/W32TIME/ PARAMETERS doesn't contain the ReliableTimeSource settings; user will have to create one. Follow steps 8- 9 otherwise proceed to step 10

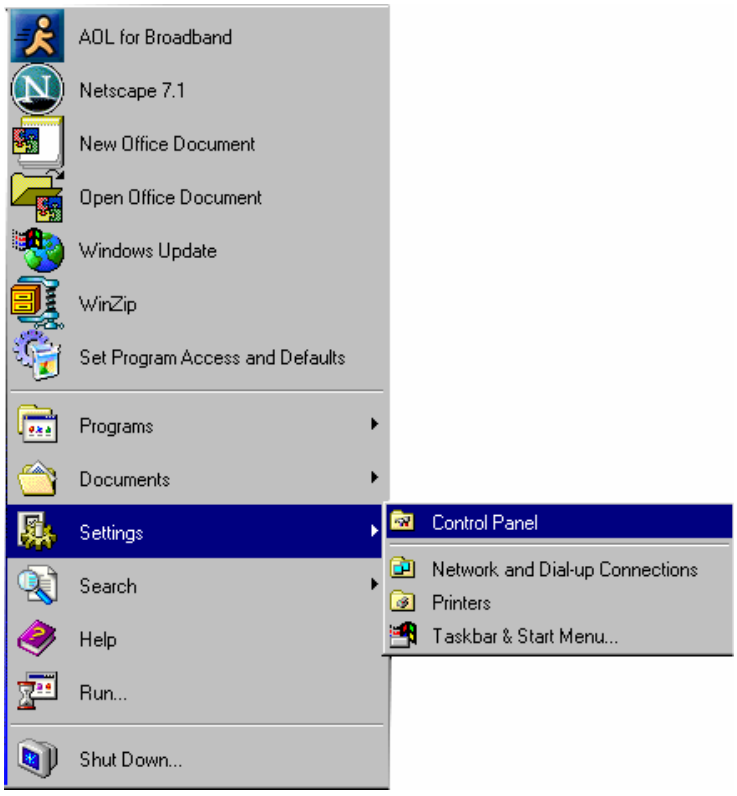
8. Right click on a empty space in the right panel and select *New/DWORD Value*.



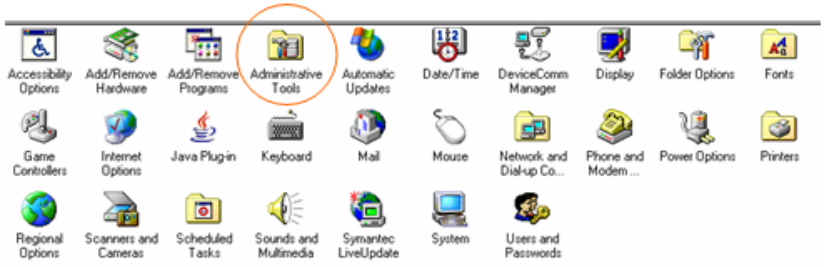
9. Key in ReliableTimeSource



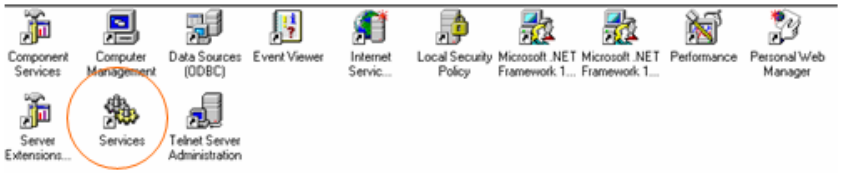
10. Click Start *Start* button and select Settings/Control Panel.



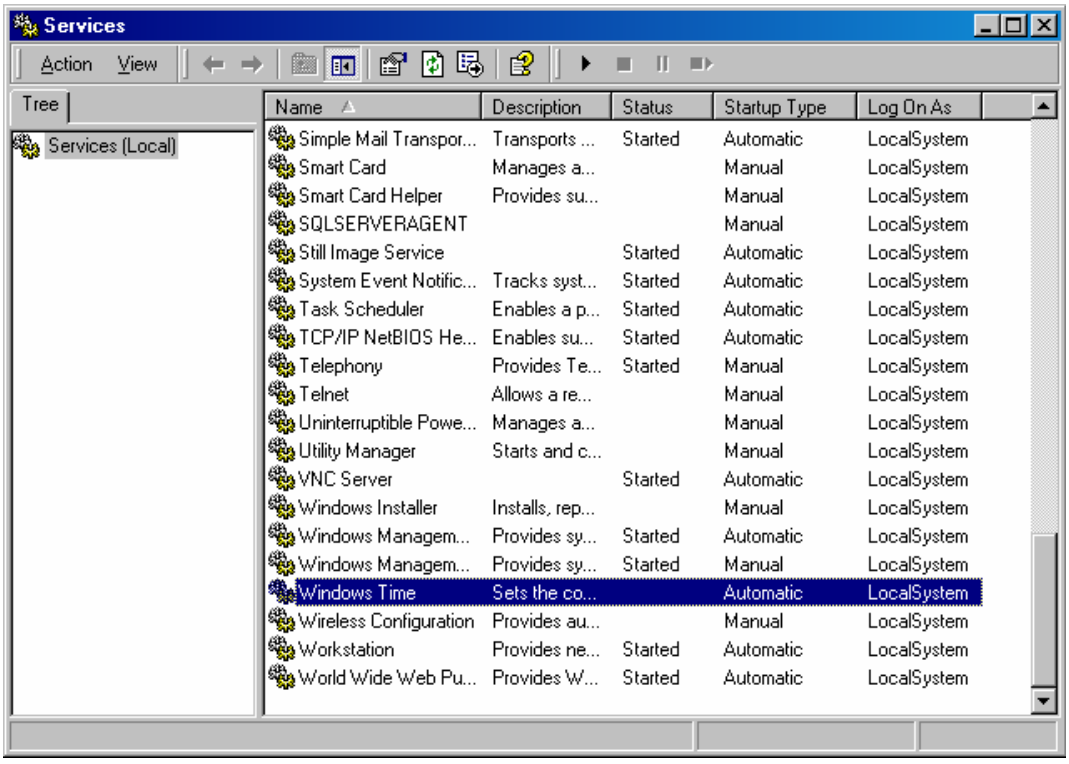
11. Double click on *Administrative Tools* icon



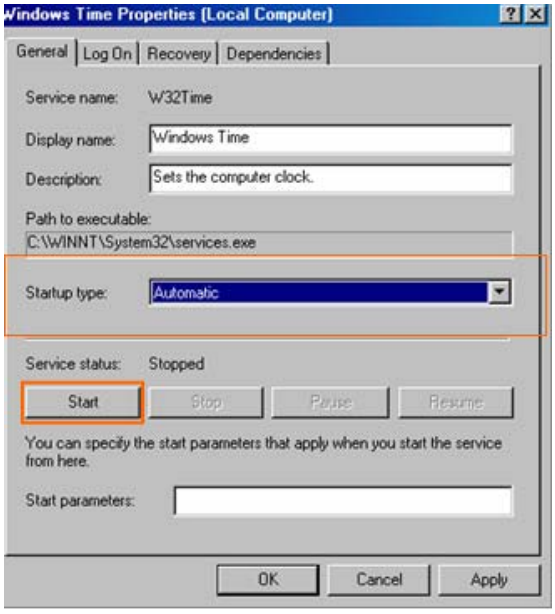
12. Double click on *Services* icon.



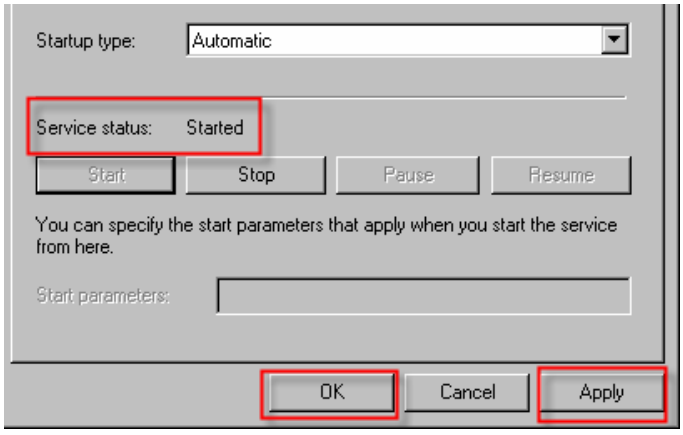
13. Scroll down to *Windows Time* and double click it.


Services
Action View
Tree
Services (Local)
Name Description Status Startup Type Log On As
Simple Mail Transpor... Transports ... Started Automatic LocalSystem
Smart Card Manages a... Manual LocalSystem
Smart Card Helper Provides su... Manual LocalSystem
SQLSERVERAGENT Manual LocalSystem
Still Image Service Started Automatic LocalSystem
System Event Notific... Tracks syst... Started Automatic LocalSystem
Task Scheduler Enables a p... Started Automatic LocalSystem
TCP/IP NetBIOS He... Enables su... Started Automatic LocalSystem
Telephony Provides Te... Started Manual LocalSystem
Telnet Allows a re... Manual LocalSystem
Uninterruptible Powe... Manages a... Manual LocalSystem
Utility Manager Starts and c... Manual LocalSystem
VNC Server Started Automatic LocalSystem
Windows Installer Installs, rep... Manual LocalSystem
Windows Managem... Provides sy... Started Automatic LocalSystem
Windows Managem... Provides sy... Started Manual LocalSystem
Windows Time Sets the co... Automatic LocalSystem
Wireless Configuration Provides au... Manual LocalSystem
Workstation Provides ne... Started Automatic LocalSystem
World Wide Web Pu... Provides W... Started Automatic LocalSystem

14. Select *Automatic* from the *Startup* Type drop down list and click *Start*.



15. Once service status is started, click *Apply* and *OK* to exit.

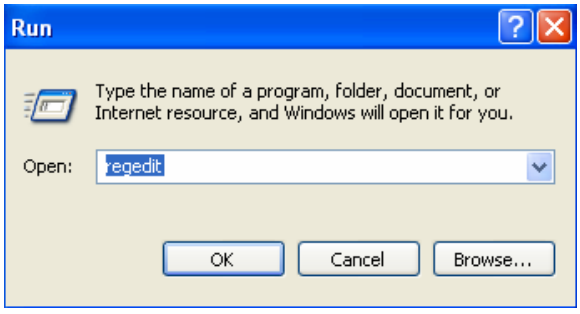


16. Reboot PC.

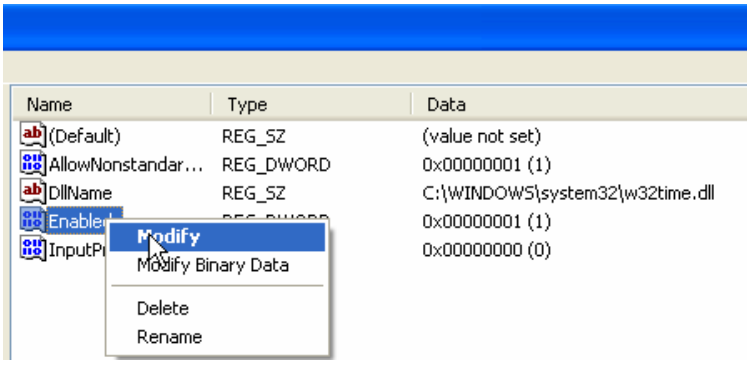
32.2 For Windows XP Professional

1. Click

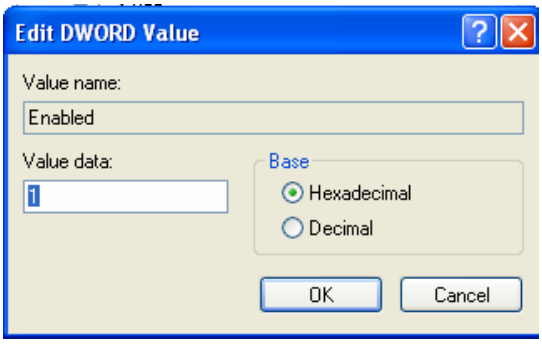
Start button and select *Run* button.
2. Type *regedit* in the window



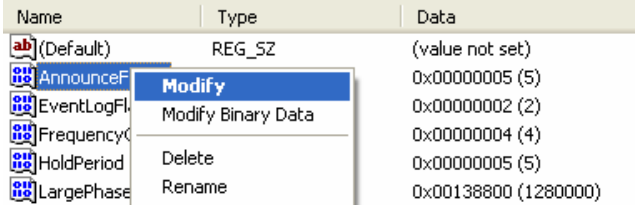
3. Select HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/SERVICES/W32TIME/TIMEPROVIDERS/NTPSERVER.
4. Right click *Enabled* and select *Modify*.



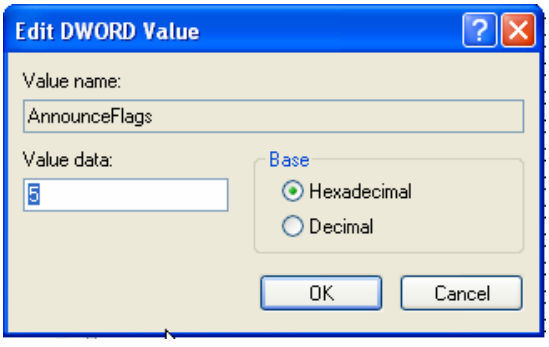
5. Enter 1 for *Value data* and click *OK*.



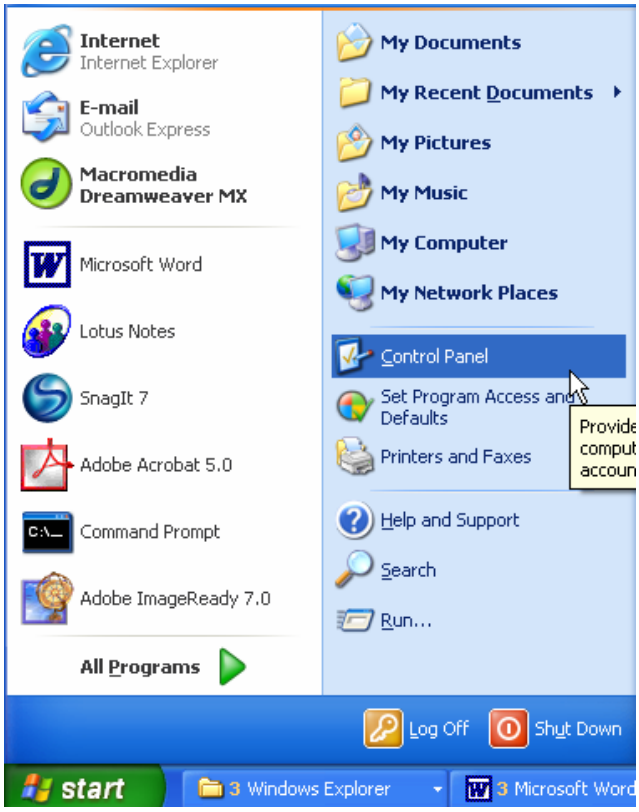
6. Select HKEY_LOCAL_MACHINE/SYSTEM/CURRENTCONTROLSET/SERVICES/W32TIME/CONFIG
7. Right click *AnnounceFlags* and select *Modify*.



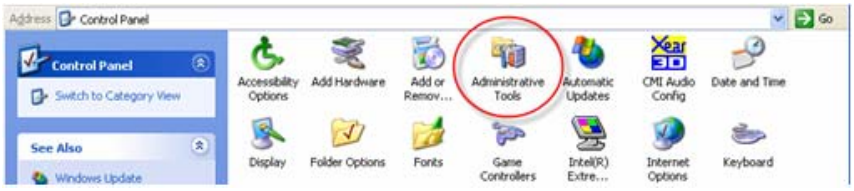
8. Enter 5 for *Value data* and click *OK*.



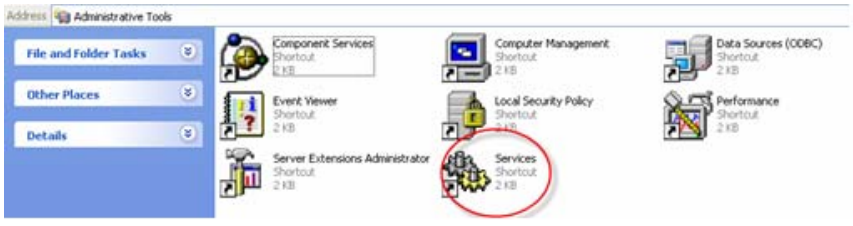
9. Click start button and select *Control Panel*.



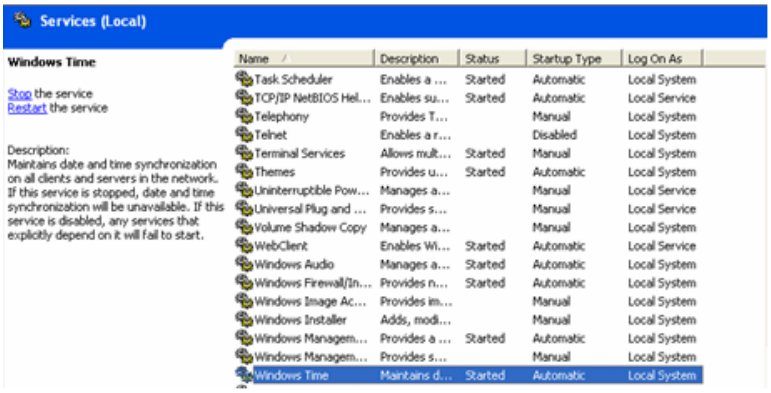
10. Double click on *Administrative Tools* icon.



11. Double click on *Services* icon.

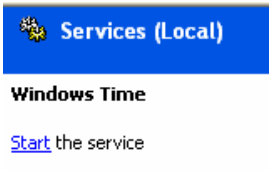


12. Scroll down to Windows Time.


Services (Local)
Windows Time
Stop the service
Restart the service
Description:
Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
Name
Description
Status
Startup Type
Log On As
Task Scheduler Enables a ... Started Automatic Local System
TCP/IP NetBIOS Hel... Enables su... Started Automatic Local Service
Telephony Provides T... Manual Local System
Telnet Enables a r... Disabled Local System
Terminal Services Allows mult... Started Manual Local System
Themes Provides u... Started Automatic Local System
Uninterruptible Pow... Manages a... Manual Local Service
Universal Plug and ... Provides s... Manual Local Service
Volume Shadow Copy Manages a... Manual Local System
WebClient Enables Wi... Started Automatic Local Service
Windows Audio Manages a... Started Automatic Local System
Windows Firewall/In... Provides n... Started Automatic Local System
Windows Image Ac... Provides im... Manual Local System
Windows Installer Adds, modi... Manual Local System
Windows Managem... Provides a ... Started Automatic Local System
Windows Managem... Provides s... Manual Local System
Windows Time Maintains d... Started Automatic Local System

13. Select *Stop the service*.

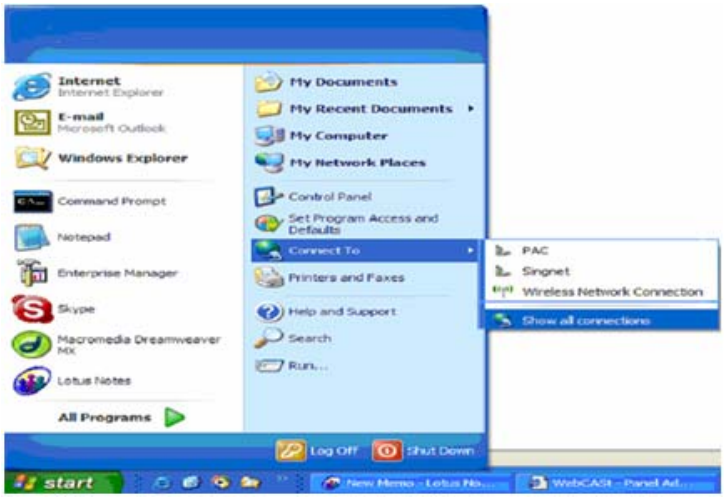
14. Once service is stop, click *Start the service*.



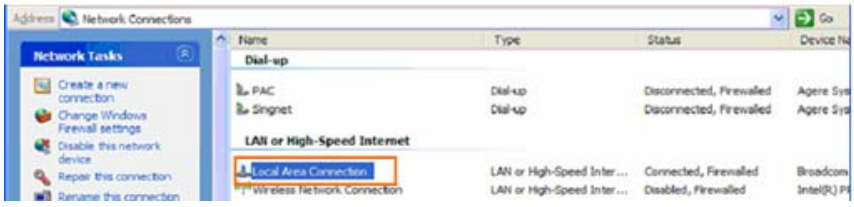
15. Reboot PC.

NOTICE!
If user is using windows XP professional with service pack 2 for the timeserver, user has to bypass the firewall protection. Follow steps 1 - 9

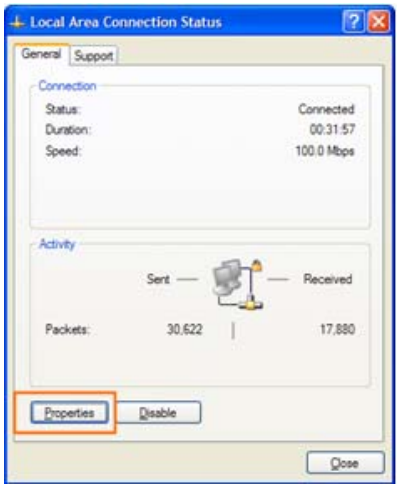
1. From the desktop, select *Start* and look for *Connect To* and select *show all connections*.



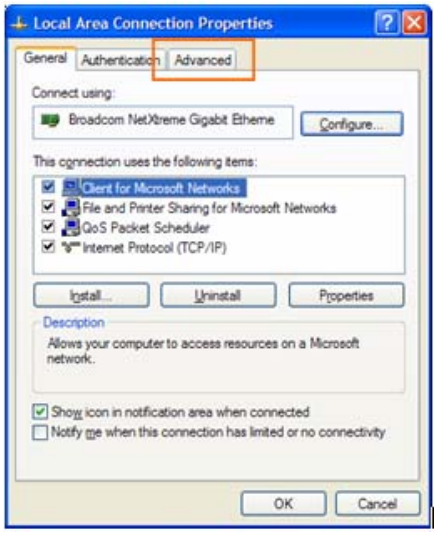
2. Click on the *Local Area Connection*.



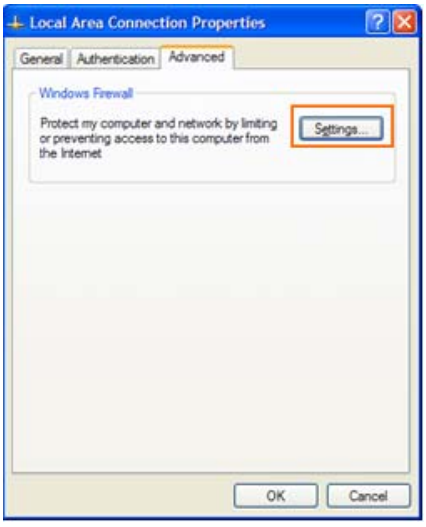
3. The following screen will appear, click on *properties*.



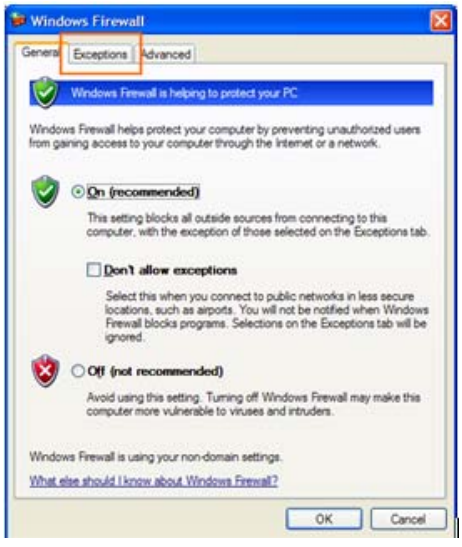
4. Click on *Advanced*.



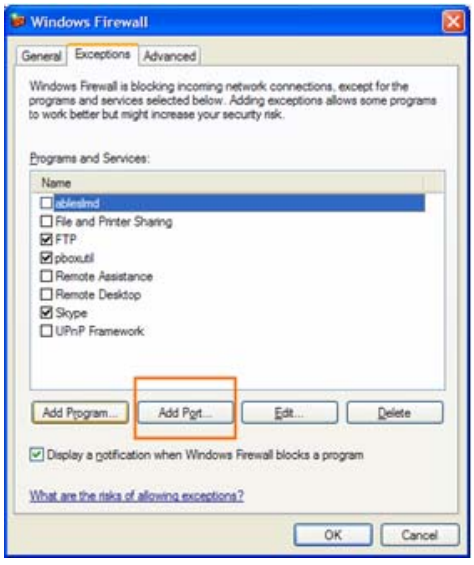
5. Click on *Settings*.



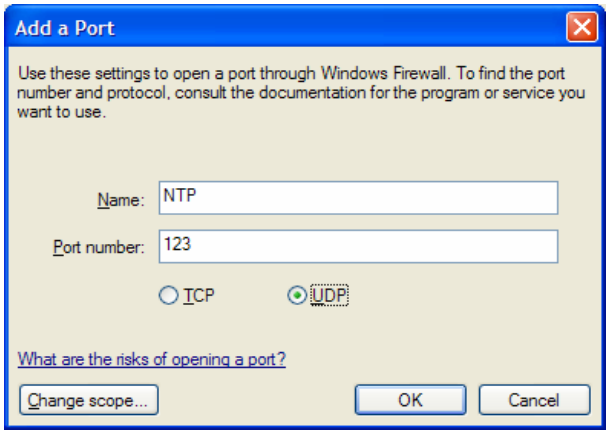
6. The below screen will appears, click on *Exceptions*.


Windows Firewall
General
Exceptions
Advanced
Windows Firewall is helping to protect your PC
Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
Windows Firewall is using your non-domain settings.
What else should I know about Windows Firewall?
OK
Cancel

7. Click on the *Add port*.



8. Enter the following data.
   Name: NTP
   Port number: 123


Add a Port
Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.
Name:
NTP
Port number:
123
TCP
UDP
What are the risks of opening a port?
Change scope...
OK
Cancel

9. Click *OK* to save the settings

33 APPENDIX F Initial Setup To Access Easy Controller

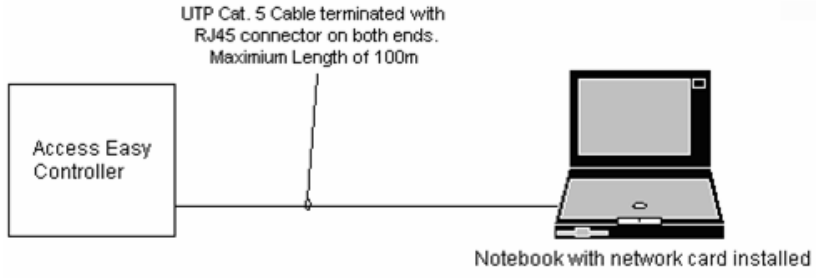
Before connection is made to Access Easy for Master, there are few conditions that must be taken into consideration. They are: -

1. If the *Central Monitoring Computer (CMC)* is not connected to a Network as in a stand-alone.
2. If the *CMC* is connected to a Network.

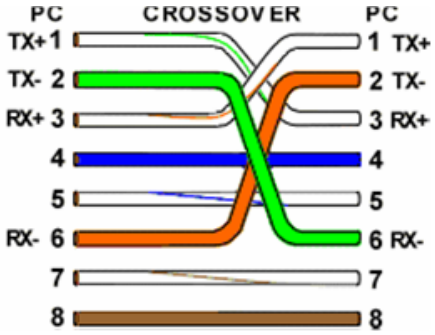
For case 1, having the CMC as a stand-alone unit, either IP Address for the for Master or CMC can be changed to suit the other.

For an initial set-up, a Notebook or a Personal Computer either stand-alone or taken from an existing network have to be used. For either case, there must be a 10Base-T Ethernet card installed and with a running web browser program such as Internet Explorer, version 4.0 and above or Netscape Navigator, version 4.0 and above.

Connect the Access Easy Controller server and Notebook using the industrial standard UTP Category 5 cable as shown below.



NOTICE!
The cable has to be terminated and polarised accordingly as shown.



The above drawing shows the *Transmit (T+ & T-)* and *Receive (R+ & R-)* lines between both end of the connectors being twisted. The wires for pins 4, 5, 7 and 8 are connected without twisting at both end of the connectors, but are not drawn above. The drawing below shows the full pin-to-pin connections with cable colour coding.

RJ45 Plug Pin (standard)	Cable Colour	RJ45 Plug Pin (twisted)
1	White/Orange	3
2	Orange	6
3	White/Green	1
4	Blue	4
5	White/Blue	5
6	Green	2
7	White/Brown	7
8	Brown	8

Hooks facing down

Hooks facing down

The individual conductors should be arranged as indicated above, taking reference to the pin numbers on the left (standard).

33.1 Procedure to set the IP Address of computer

This section provides procedure to set the IP Address for the PC and Macintosh.

33.1.1 For PC Users

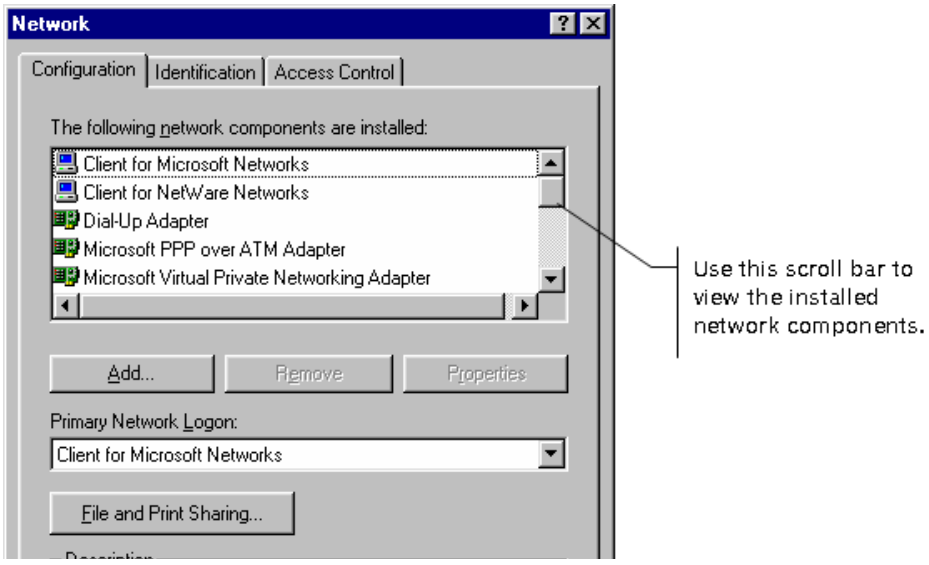
Follow through the procedures to set the IP Address of the PC.

NOTICE!

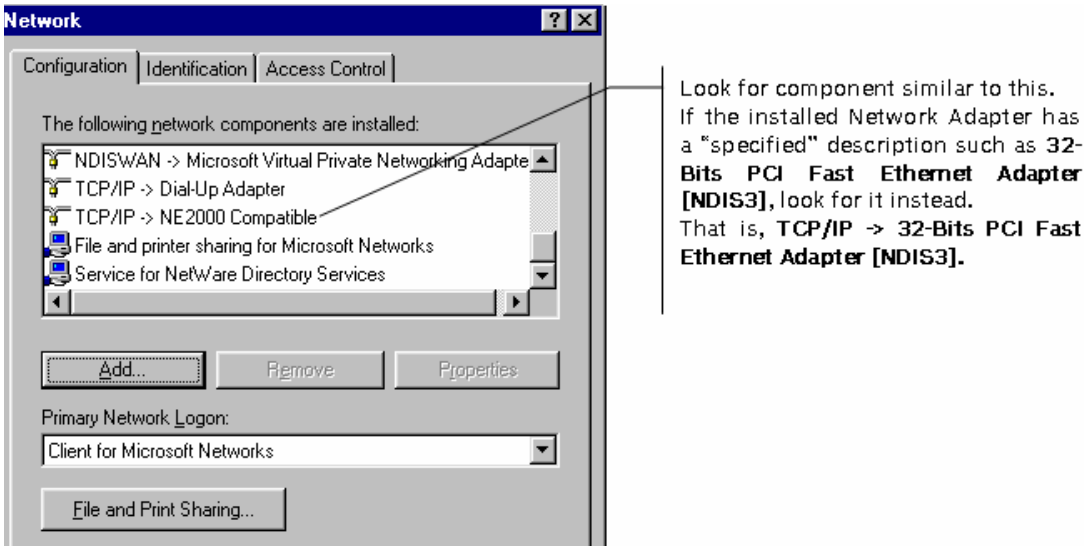
The example described here is based on Windows 98 and Internet Explorer 5. Differences might appear for the dialog box, displays, or description if other version or different operating system is used. However, the principle of setting is the same.

1. Click on the Start button, followed by Settings | Control Panel.

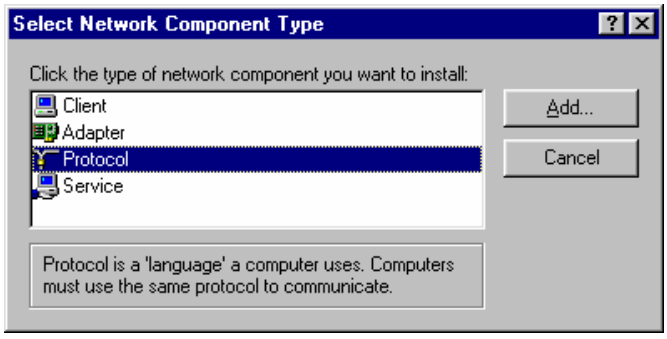
2. Double-click on the Network icon, the Network dialog box appears.



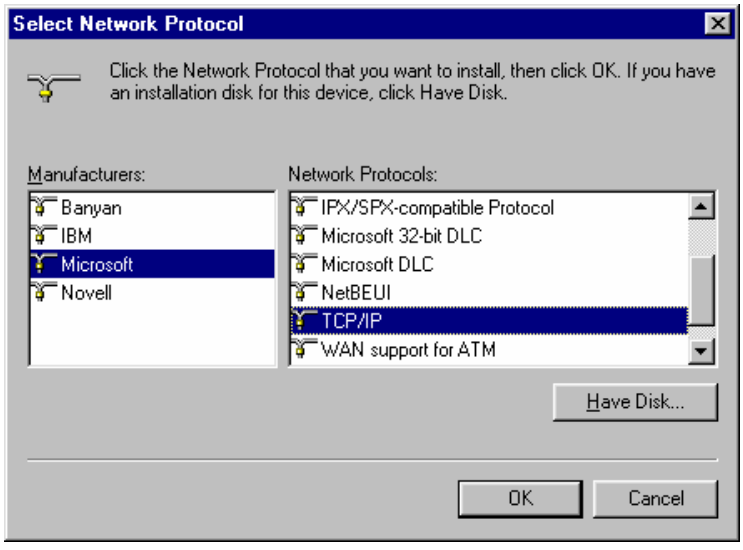
3. Use the *Scroll Bar* to look up for *TCP/IP* from the list as shown in the following diagram. However if this component is not found, proceed from step 4 to step 7 to install it, else skip to step 8.


Network
Configuration
Identification
Access Control
The following network components are installed:
NDISWAN -> Microsoft Virtual Private Networking Adapte
TCP/IP -> Dial-Up Adapter
TCP/IP -> NE2000 Compatible
File and printer sharing for Microsoft Networks
Service for NetWare Directory Services
Add...
Remove
Properties
Primary Network Logon:
Client for Microsoft Networks
File and Print Sharing...
Look for component similar to this.
If the installed Network Adapter has a "specified" description such as **32-Bits PCI Fast Ethernet Adapter [NDIS3]**, look for it instead.
That is, **TCP/IP -> 32-Bits PCI Fast Ethernet Adapter [NDIS3].**

4. To add the TCP/IP component, click on the **Add** button. The Select *Network Component Type* dialog box appears.



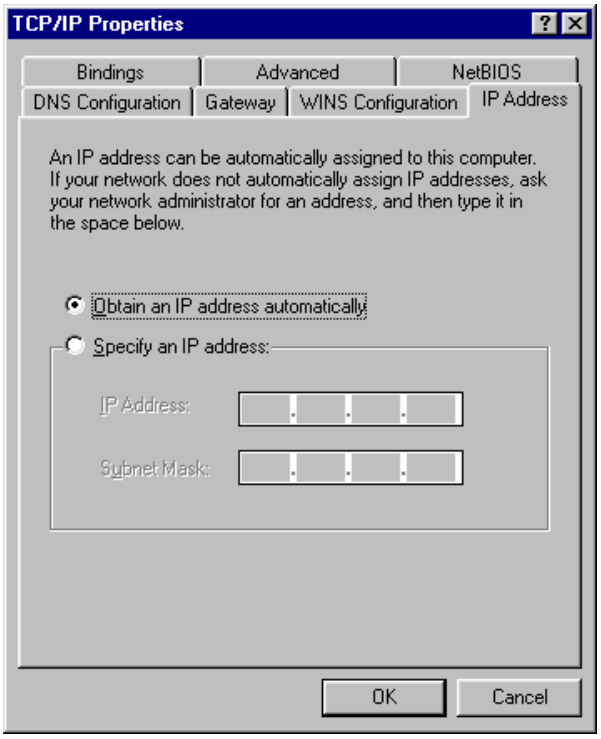
5. Click on component type Protocol and click on the **Add** button. The *Select Network Protocol* dialog box appears.
6. Click on *Microsoft* and *TCP/IP* as shown below.



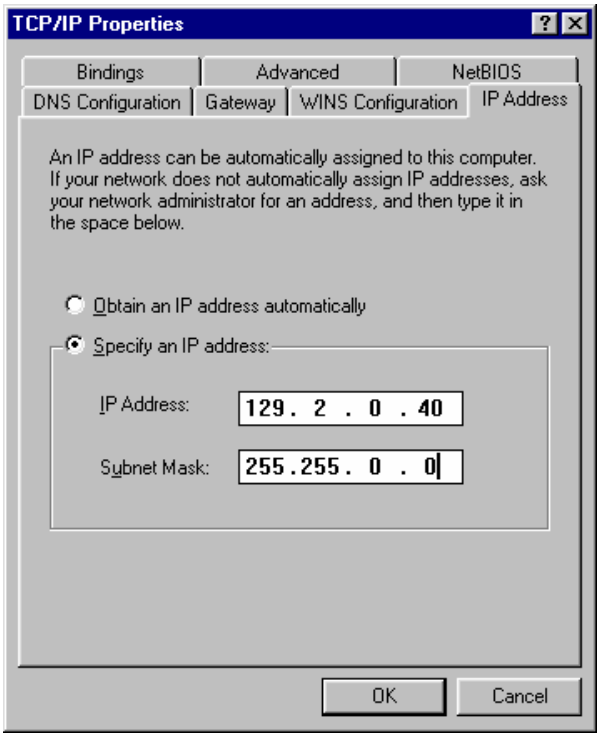
7. Click on the **OK** button to proceed with the component installation. Follow through the on-screen instruction to complete.

NOTICE!
You might be required to have your Windows Installation Disk in your CD ROM drive.

8. Continuing from step 3, click on the **Properties** button. The *TCP/IP Properties* dialog box appears.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

9. Click on the *Specify an IP address* radio button. This will enable the field for *IP Address and Subnet Mask*.
10. Enter the *IP Address and Subnet Mask* as shown. This will be the PC's IP Address for this initial set-up.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
129. 2 . 0 . 40
Subnet Mask:
255.255. 0 . 0
OK
Cancel

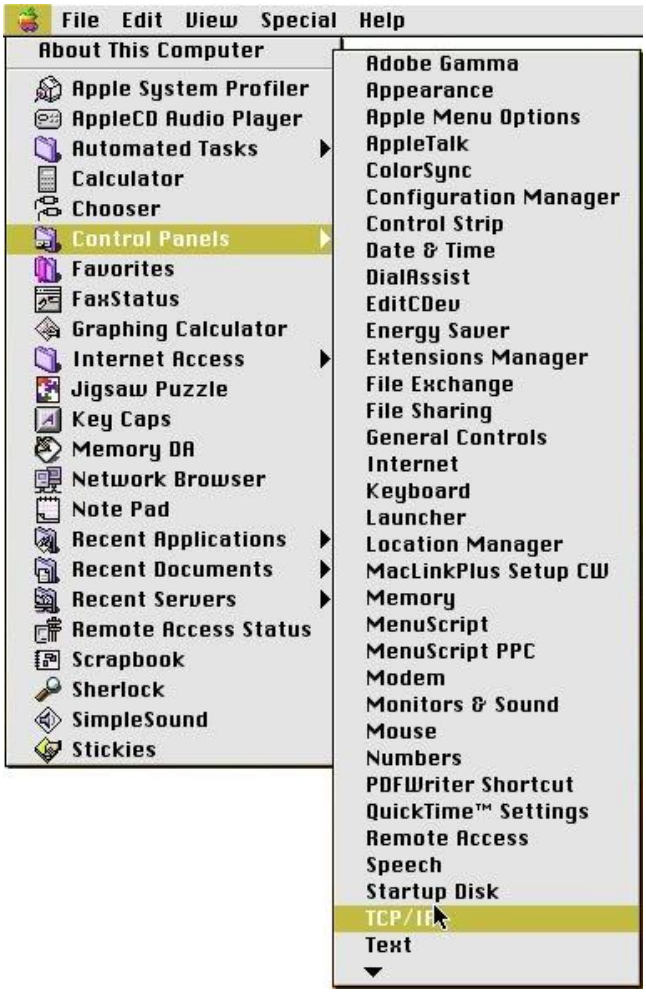
11. Click on **O**K button.
12. Reboot the computer in order for the setting to take effect.

33.2 For Macintosh Users

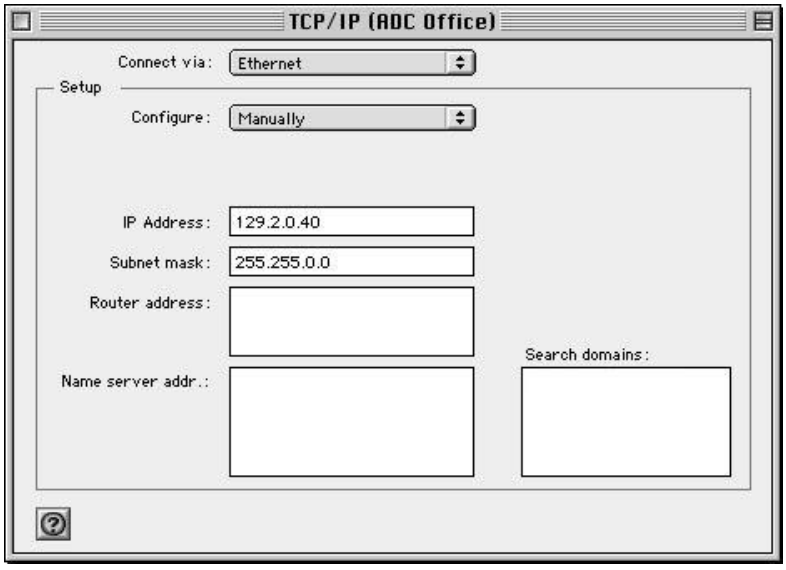
Follow through the procedures to set the IP Address for the Macintosh.

1. Click on the Apple icon to show a list of control function.
2. Select Control Panels, TCP/IP

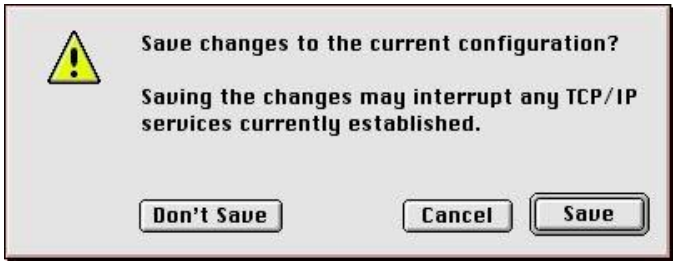
The *TCP/IP* dialog box appears



3. Enter the *IP Address* and the *Subnet mask* as shown below. This will be the Macintosh's IP Address for this initial set-up.



4. Click on the **Save** button when prompted. This message will appear when you attempt to close the dialog box.


Save changes to the current configuration?
Saving the changes may interrupt any TCP/IP services currently established.
Don't Save
Cancel
Save

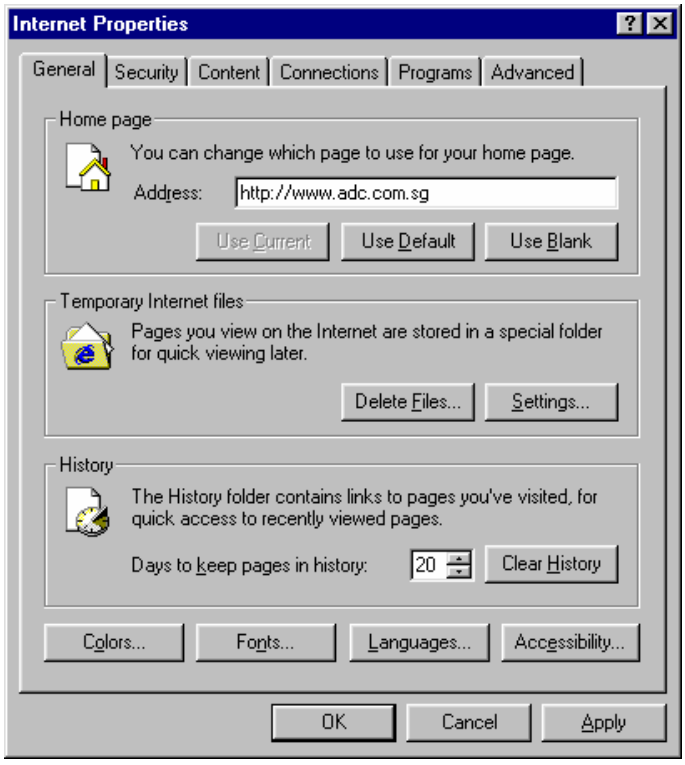
33.3 Setting to be made to the Web browser

33.3.1 For PC User

Follow the procedure to set up the Web browser options.

1. From the *Windows Control Panel*, click on the

icon. The Internet Options dialog box appears.



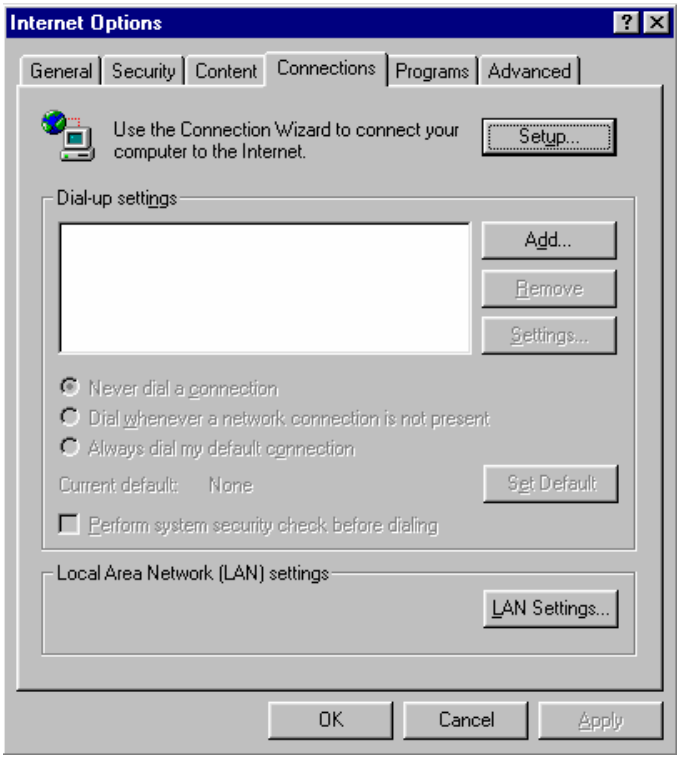
2. If you wish to show the Access Easy for Master *Login page* every time you activate your web browser program, then change the *Home page* Address to the Access Easy for Master *assigned IP address* (see NOTICE) else, leave it as what was defined previously.

NOTICE!
The Network Administrator should assign the IP Address if the Access Easy for Master is to be connected to the Network.

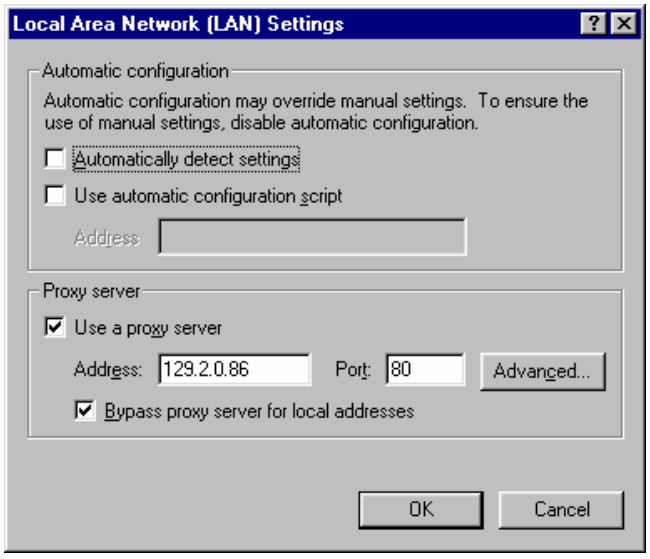
3. Under the *Temporary Internet files* heading, click on the **Settings** button to go into the next dialog box. Confirm that the *Check for newer versions of stored pages* is set to *Every visit to the page*, as shown in the following diagram. If it is not, click on the corresponding radio button.

   This step is necessary in order for the view in View Activity to be updated periodically.

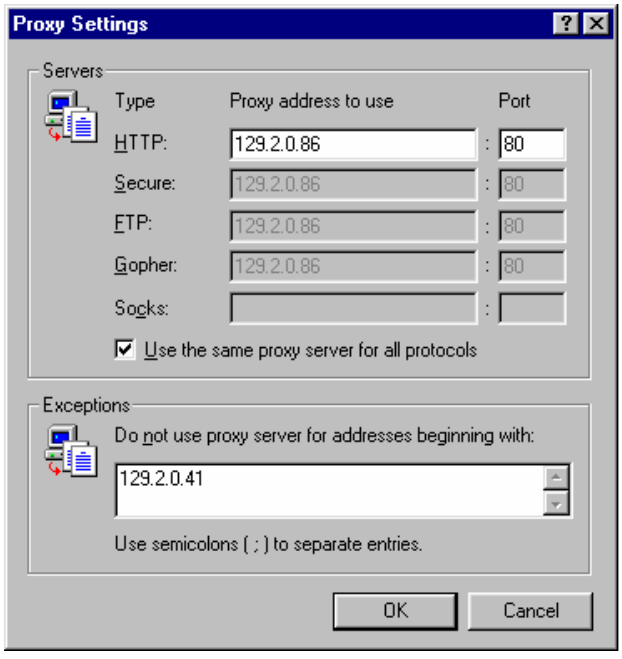
4. Click on the **OK** button to exit to previous dialog box.



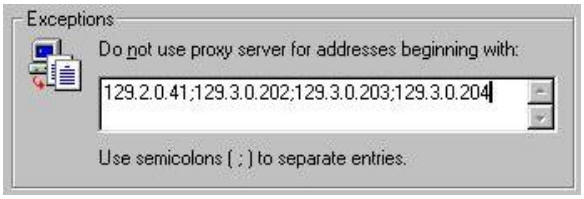
5. Under the **Connections tab**, click on the **LAN Settings** button The *LAN Settings* dialog box appears.



6. Click on the **Advanced** button. The *Proxy Settings* dialog box appears.



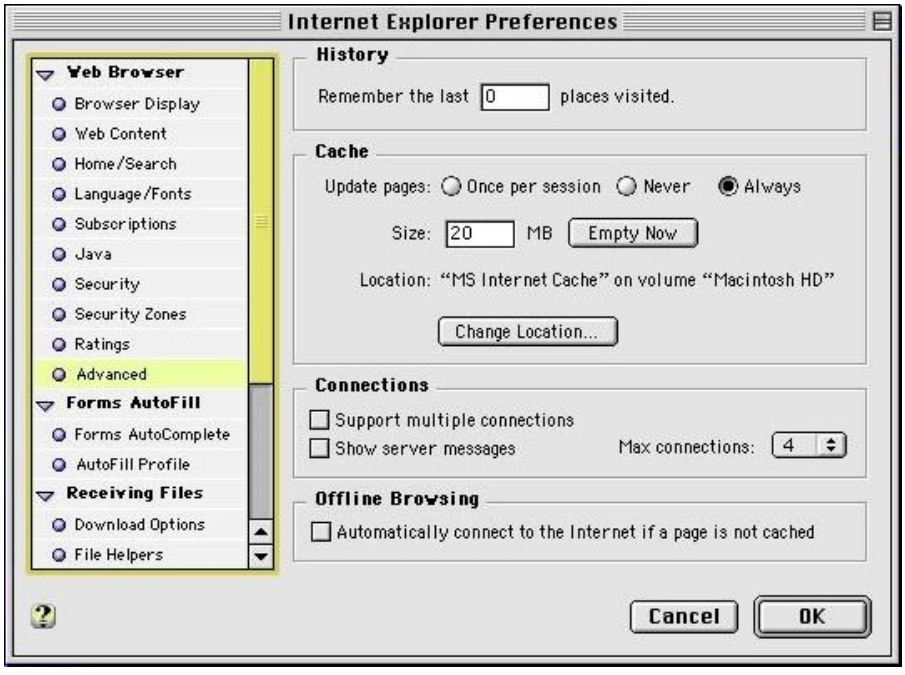
7. Enter the default *IP address* for the Access Easy for Master in the *Exceptions* edit field as shown above.
8. If the IP Address of the Access Easy for Master(s) has been assigned, continue to enter the address in the Exceptions edit field, separate each Address by a semicolon [;]. The next screen-capture shows the Default IP Address for Access Easy for Master and three assigned Access Easy for Master IP Addresses, 129.3.0.202, 129.3.0.203 and 129.3.0.204.


Exceptions
Do not use proxy server for addresses beginning with:
129.2.0.41;129.3.0.202;129.3.0.203;129.3.0.204
Use semicolons (;) to separate entries.

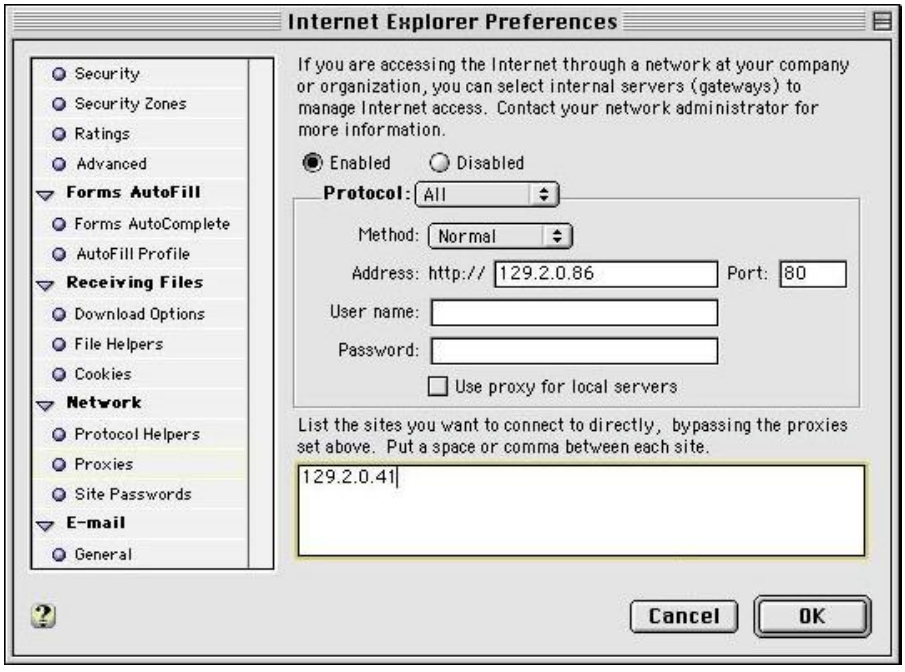
9. Click on the **OK** button repeatedly to exit the I*nternet Options* setting.
10. Close the *Control Panel*.

33.4 For Macintosh Users

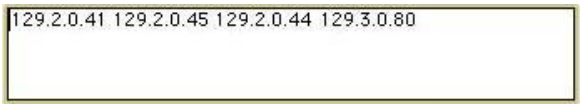
1. Launch the Internet Explorer for Macintosh.
2. From the Toolbars, click on **Preferences**.
3. Under **Web Browser**, select *Advanced* (see diagram below).
4. Select Update pages - Always for **Cache**.



5. Use the Scrollbar to scroll down the listing to look for *Proxies*.



6. Enter the Access Easy for Master default IP Address into the box as shown above. IP Addresses enter here will bypass the proxies and connect directly.
7. If the IP Address of the Access Easy for Master(s) has been assigned, continue to enter the address in the field, separate each Address by a space or a comma. The screen-capture shows the Default IP Address for Access Easy Controller and three assigned Access Easy for Master IP Addresses, 129.2.0.45, 129.2.0.44, and 129.3.0.80.



8. Click on the **OK** button to close the dialog box.

With this settings done, we can proceed to access the Access Easy for Master.

Now run the Web Browser program from Windows /Macintosh.
Enter the Access Easy for Master default URL address as shown.

NOTICE!
As the current configuration has no connection to the network or modem, accessing an Internet address is not possible. An error message will appear, a sample of which is shown below.

Enter default URL Address for
Access Easy for Master
Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://129.2.0.41/
Go
Back Forward Stop Refresh Home Search Favorites History Mail Print
The page cannot be displayed
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.
Please try the following:

1. Press the **Enter** key or click on the Go button. This should bring you to the *Access Easy* for Master *User Login* page.
2. Proceed with the *Login* (see the following NOTICE).

NOTICE!
If the Access Easy Controller is connected to the Central Monitoring Computer via a hub, as in a Network configuration, the UTP Cat. 5 cable connecting the Access Easy Controller and the hub must be polarised accordingly as shown on the following drawing.

RJ45 Plug Pin (standard)	Cable Colour	RJ45 Plug Pin (One-to-One)
1	White/Orange	1
2	Orange	2
3	White/Green	3
4	Blue	4
5	White/Blue	5
6	Green	6
7	White/Brown	7
8	Brown	8

Hook facing down

Hook facing down

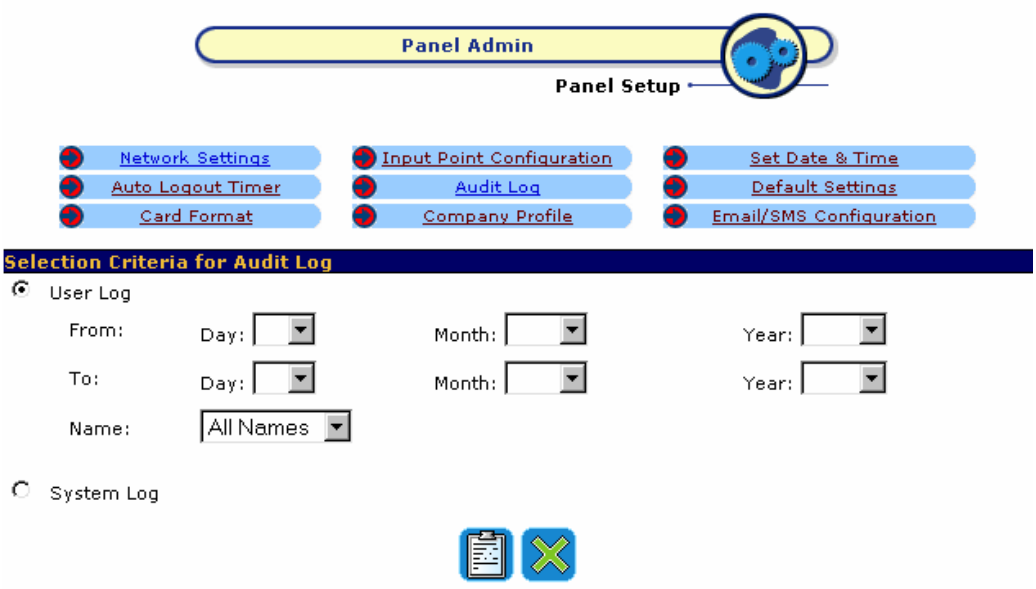
33.5 Setting the Access Easy Controller IP Address Through Address Resolution Protocol (ARP)

An address is a set of unique numbers by which you identify your PC or Access Easy Controller.

A mac address is the hardware address of the network device.

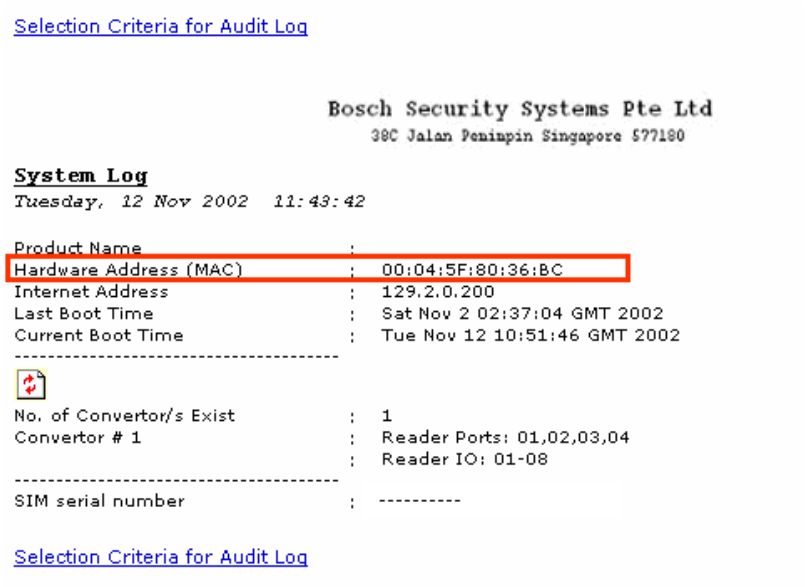
With the help of the arp command, the address of the Access Easy Controller can be customised according to your network. You need not know the previous address of your Access Easy Controller to use the arp command, but you will need to know the mac address of the Access Easy Controller . The mac address is listed in the System Audit log of the Access Easy Controller. To find out the mac address, you will need to first log in to the Access Easy Controller and follows the steps as shown on the following page:

Click on *Panel Admin* at the Home page of the Access Easy for Master.
Click on *Panel Setup* on the left panel menu selection.
Click on *Audit Log* to bring you to the page as shown in the following.



Check the System Log radio button and click the list button to shows the report.

The following shows the report generated, take note of the Hardware address, which is the mac address that we need.



Selection Criteria for Audit Log

Bosch Security Systems Pte Ltd
30C Jalan Pemimpin Singapore 577180

System Log
Tuesday, 12 Nov 2002 11:43:42

Product Name	:	
Hardware Address (MAC)	:	00:04:5F:80:36:BC
Internet Address	:	129.2.0.200
Last Boot Time	:	Sat Nov 2 02:37:04 GMT 2002
Current Boot Time	:	Tue Nov 12 10:51:46 GMT 2002
No. of Convertor/s Exist	:	1
Convertor # 1	:	Reader Ports: 01,02,03,04
	:	Reader IO: 01-08
SIM serial number	:	----------

Selection Criteria for Audit Log

With the mac address, we could now use arp to change the IP address of the Access Easy for Master. From any of your remote PCs, issue the following commands from the command prompt.

If you are using Windows NT or Windows 98

arp-s <new address you want to specify for your Access Easy for Master> <mac address of your Access Easy Controller>
ping <new address you have just set> to check connectivity to the Access Easy Controller.

for example : if you want to change the address of your Access Easy for Master to 129.3.0.99 and the mac address of your Access Easy Controller is 52-54-4c-0-0-2c, the command will be :

arp -s 129.3.0.99 52-54-4c-0-0-2c
ping 129.3.0.99

If you are using Windows 95

arp-s <new address you want to specify for your Access Easy for Master> <mac address of your Access Easy Controller > <address of your PC>
ping <new address you have just set>

for example : if you want to change the address of your Access Easy for Master to 129.3.0.99 and the mac address of your Access Easy Controller is 52-54-4c-0-0-2c and the address of your PC is 129.3.0.77, the command will be :

arp -s 129.3.0.99 52-54-4c-0-0-2c 129.3.0.77
ping 129.3.0.99

If you are using Unix/Linux and OS/2

arp-s <new address you want to specify for your Access Easy for Master> <mac address of your Access Easy Controller > temp
ping <new address you have just set>

for example: if you want to change the address of your Access Easy for Master to 129.3.0.99 and the mac address of your Access Easy Controller is 52-54-4c-0-0-2c , the command will be :

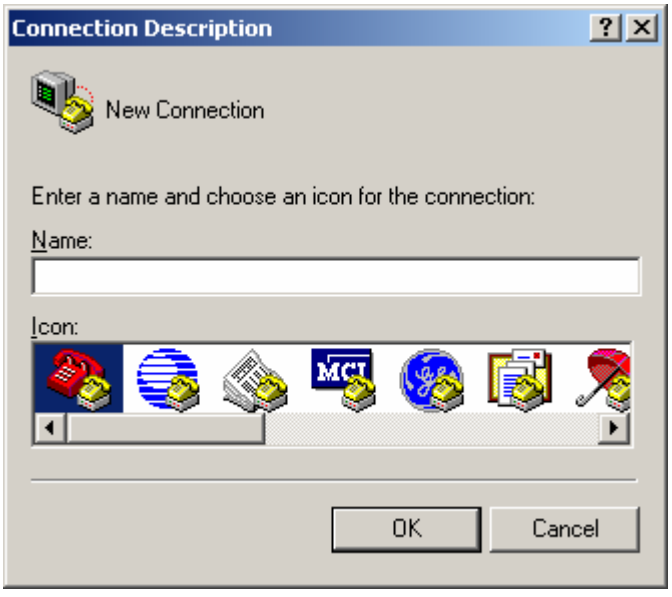
arp -s 129.3.0.99 52-54-4c-0-0-2c temp
ping 129.3.0.99

After you have issue the ping command to the Access Easy Controller, it should reboot. After it has rebooted, it will resume operation using the new IP address that you have set.

34 APPENDIX G

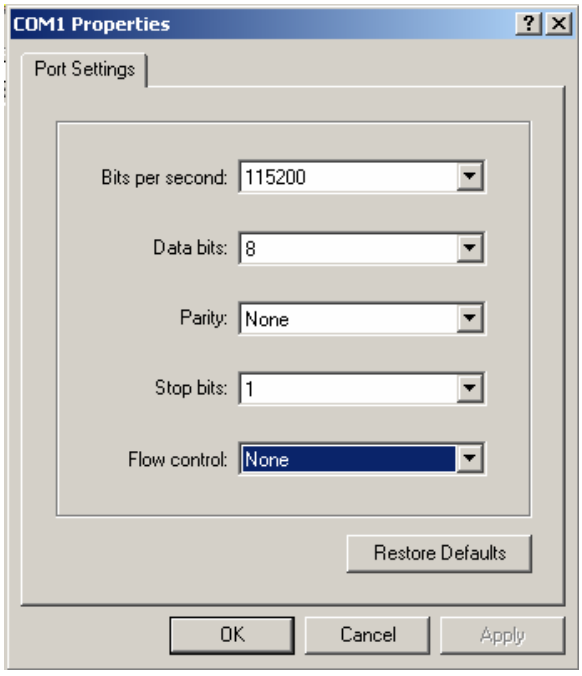
34.1 Preparing the WAVECOM GSM Modem for Access Easy Controller

1. Insert the SIM Chip into the GSM Modem.
2. Power up the GMS modem
3. Connect the PC serial port and the Modem using the serial cable that comes with the Modem.
4. Please run the HyperTerminal program from the Windows. Go to Program > Accessories > Communication > HyperTerminal.
5. You will be prompted to enter the name of the connection, please enter any name.



6. Select the COM port that the GSM Modem is connected to.

7. Click *OK* and you will go to the screen to set the Baudrate, set it to to *115200bps*, *8bit data, 1 stop bit and no parity*.



8. Click *OK* button to start the connection.

NOTICE!

Once connected, you should check whether the connection is stable by typing *"AT"* follow by enter, you should get an *"OK"* reply from the GMS modem.

If there is no reply or the reply is not *"OK"* but display some unknown character, then it is possible that the GSM Modem baudrate is incorrect. Change the baudrate and reconnect.

9. Once you have connected to the GMS Modem, you shouldn't change the baudrate.
10. Type *"AT+IPR=19200"* and press the <Enter> key. You should get an *"OK"* reply.
11. Now you will need to change your baudrate of the HyperTerminal to 19200.
12. Click this icon to disconnect the connection.
13. Click on the icon to change the Baudrate to 19200 and then click on the icon to reconnect with the GSM modem again.
14. Type *"AT"* and follows by a return, if the GSM modem replies you *"OK"* then the configuration is complete.
15. You will need to save the configuration into the non -volatile memory in the GSM modem.
16. Type *"AT&W"* and follows by a return, the GSM modem will reply you *"OK"*.
17. Reboot the GSM modem and try connecting again to the GMS modem using the baudrate 19200.

34.2 How to test the GSM modem

You could test whether the GSM modem is working before connecting it to the AEC.

1. Firstly prepare the GSM Modem as shown above, and then connect the GSM Modem to the PC via the serial port and runs HyperTerminal. Follows the below steps to send out a test SMS.

   Type *"AT+CMGS=xxxxxxxx"* follows by a return, you will expect to see a *">"* reply from the GSM Modem. (xxxxxxxxx denote the mobile number)

2. Next type the message *"TESTING TESTING"* follows by *<Ctrl> + <Z>* follows by a return, you will expect to see a *"+CMGS: nn"* follows by a *"OK"*, this means the SMS is sent successfully. (nn denote a double digit number provided by the GSM modem).

NOTICE!
Models supported by AEC: Wavecom M1306B

Robert Bosch (SEA) Pte Ltd
11 Bishan Street 21
573943 Singapore
Singapore
www.boschsecurity.com
© Robert Bosch (SEA) Pte Ltd, 2012